United Nations A/66/151

General Assembly

Distr.: General
18 July 2011

Original: English

Sixty-sixth session
Item 131 of the provisional agenda*
Financial reports and audited financial statements, and reports of the Board of Auditors

Progress in the implementation of the International Public Sector Accounting Standards

Note by the Secretary-General

The Secretary-General has the honour to transmit to the General Assembly a letter dated 14 July 2011 from the Chair of the United Nations Board of Auditors transmitting the report of the Board of Auditors on the progress in the implementation of the International Public Sector Accounting Standards as at 30 June 2011.

* A/66/150.

11-41885 (E) 160811

Please recycle

Letter of transmittal

12 July 2011

I have the honour to transmit to you the report of the Board of Auditors on the progress in the implementation of the International Public Sector Accounting Standards as at 30 June 2011.

(*Signed*) **Liu** Jiayi
Auditor-General of the People's Republic of China
Chair of the United Nations Board of Auditors

The President of the General Assembly
of the United Nations
New York

Report of the Board of Auditors on the progress in the implementation of the International Public Sector Accounting Standards

Summary

In November 2005, the High-level Committee on Management of the United Nations System Chief Executives Board for Coordination made the landmark recommendation that United Nations system organizations move from the internally developed United Nations System Accounting Standards and adopt the International Public Sector Accounting Standards (IPSAS) for the presentation of the organizations' financial statements.

IPSAS are accruals-based standards, written specifically for the public sector and international organizations. Accruals accounting means that an organization recognizes costs when they are incurred and income when it is earned, and must account for the value, the volume and the location of all of its assets and liabilities. This improved information will provide Member States with greater insights into entities' performance and financial position, and management with better information to maintain control, drive cost-effective decision-making, and secure long-term financial sustainability.

In the light of implementation delays, the imminent deadlines for many entities, and the concerns previously expressed by the Board of Auditors, the Advisory Committee on Administrative and Budgetary Questions recommended that the Board prepare an annual report on progress in IPSAS implementation (see A/65/498). Building on its previous work, the Board examined progress by the United Nations (including peacekeeping operations) towards its 2014 implementation target and by a range of other funds and programmes within its portfolio towards their 2012 target. This first IPSAS progress report by the Board sets out the findings and conclusions from that work. The table at the end of this summary provides an overview of the Board's findings across all entities.

Overall conclusion of the Board

There are a number of critical risks to achieving IPSAS implementation on time and to realizing the benefits envisaged by the General Assembly when it took the decision to adopt IPSAS. Unless urgent and effective action is taken to address these risks, it is highly unlikely that IPSAS will be successfully implemented on target within the United Nations, its peacekeeping operations and its funds and programmes. The Board is concerned that there must be no further deferment of the existing deadlines.

For the United Nations and the peacekeeping operations, the Board welcomes the increased focus on practical IPSAS implementation. There is a need to urgently decide on the realistic prospect of a revised enterprise resource planning (Umoja) implementation strategy in support of IPSAS implementation in 2014; and then to develop and roll out a practical and detailed IPSAS implementation plan across all operational areas if the huge task of gathering and cleansing the accounting data is to be achieved. This is a particularly high risk for the United Nations and peacekeeping operations, given the absence of a detailed implementation plan, the scale, the

number and the complexity of the entities involved, and the uncertainties over the implementation of Umoja.

In the Board's view, implementation on target (by 2012) is possible for all of the remaining entities, but there are significant and pressing risks to be managed if they are to achieve this. The Board is particularly concerned about progress to date by the United Nations Joint Staff Pension Fund, which is yet to obtain approval of its Pension Board to continue applying the Financial Regulations and Rules "mutatis mutandis" to its accounting and financial reporting process in a manner that allows it to be IPSAS-compliant by 2012. The Board is also concerned about the entities with implementation targets for 2012 that have not yet finalized their accounting policies.

While important to accountability and transparency, the achievement of unmodified audit opinions alone will not signal successful IPSAS implementation. It is the benefits to improved decision-making and more cost-effective delivery that are important. Securing these benefits will require engagement across all operational areas and significant cultural change. The Board recognizes that delivery of the full benefits from IPSAS adoption for financial reporting purposes and accrual accounting for management purposes will not be delivered immediately but will come from careful management over time. The Board is concerned that benefits realization plans are absent in nearly all entities and that appropriate change management arrangements are not yet in place to achieve the necessary business and cultural transformation. The Board has seen little evidence that operational areas understand the new information that will be available to them through IPSAS, or are considering and preparing for how they will use it to improve the cost-effectiveness of their operations.

Therefore, even if IPSAS-compliant financial statements are delivered by the target dates, there remains a significant risk of considerable delays before the full benefits from adopting accruals accounting under IPSAS are realized.

To realize the full benefits of the new processes and information under IPSAS, there also needs to be clear and effective organizational accountability and risk management frameworks that align both the appropriate accountability and authority against those managers responsible for delivering the core services and mandates of their organizations. The Board is concerned that without an appropriate accountability framework, within the United Nations in particular, managers will not be empowered or held accountable for using the new information to deliver more cost-effective operations and services.

Key findings on the United Nations and its peacekeeping operations: implementation target 2014

Inter-dependency with Umoja

The IPSAS adoption strategy selected by the United Nations and its peacekeeping operations is dependent on the successful implementation of Umoja, which, in addition to many other benefits, will provide the systems necessary to process increased data requirements under IPSAS. Delays with the Umoja project mean that it will now not be completed in time to support IPSAS as envisaged, and the Board is yet to see any firm plans on how the Umoja project will be reprioritized to support IPSAS implementation. Should the reprioritization of Umoja prove impossible, or only partially possible, there is currently no firm contingency plan in

place, but the Board recognizes the United Nations and peacekeeping operations are aware of and beginning to address this risk.

Risks to implementation

Until a decision has been made on Umoja, and the Administration has prepared a clear overarching implementation plan setting out the full timetable implications, it is not possible for the Board to provide any firm assurance that the United Nations is on track to deliver IPSAS adoption by 2014. Regardless of the outcome of the decision, the Board notes further significant risks to achieving the target date:

- Effective risk management of IPSAS adoption is now crucial. At the time of the Board's review, there was no formal risk management framework for the project, though the Administration has subsequently informed the Board that a risk register has since been put in place;
- The significant exercise needed to gather data to value assets and arrive at meaningful opening balances is not well advanced and many operational areas are not yet primed to undertake the task. The successful completion of the exercise will require concerted efforts from the whole organization;
- The United Nations IPSAS Implementation Project Team is not confident that it has the resources to prepare "dry run" financial statements with real accounting data. Without a "dry run" in the year prior to IPSAS implementation it is unlikely that an organization as complex as the United Nations will be able to establish opening balances for asset values in the balance sheet and achieve financial statements of sufficiently high quality to withstand audit within the planned implementation time frames;
- There will be insufficient time for operational areas to be ready to implement the policies and the associated processes correctly and consistently. Given the scale of peacekeeping operations in particular, this is a serious risk to achieving compliant financial statements in the first year of implementation.

Benefits and change management

The Board has seen little evidence of the deployment of the change management resources and methodologies needed to support IPSAS implementation and tackle the cultural changes needed to embed accruals-based concepts; for example, the need for non-financial staff to recognize the importance of reporting the progress of procurement from the point of placing an order to receiving the goods, receiving the invoice and then making final payment. More could be done to integrate the change management activities for the IPSAS and Umoja projects.

Key findings on the United Nations funds and programmes: implementation target 2012

The findings below relate to the Board's examination of the progress on IPSAS implementation at the United Nations Development Programme (UNDP), the United Nations Population Fund (UNFPA), the United Nations Office for Project Services (UNOPS), the United Nations Children's Fund (UNICEF), the Office of the United Nations High Commissioner for Refugees (UNHCR), the United Nations Relief and Works Agency for Palestine Refugees in the Near East (UNRWA) and the United

Nations Joint Staff Pension Fund. In the Board's view, implementation on target is possible for all of these entities, but the Board has the following key concerns:

- Despite the 2012 deadline, most organizations have not finalized all accounting policies, and significant work remains to adequately collect, cleanse and migrate data for IPSAS implementation, with uncertainty about how big this task might be in some cases. The Board is concerned that delays in the completion of accounting policies may have the effect that field offices at the entities might not be trained and familiar with the new policies and procedures necessary for IPSAS implementation; for example, the need to accurately catalogue the volume and value of assets;
- While most entities are planning to develop "dry run" statements prior to implementation using real accounting data, the Board is concerned that the timetable for this is now very challenging and any delays could leave inadequate time for review and correction;
- Fully resourced and expert implementation teams are not in place in most entities. UNRWA lacks a specific project leader or dedicated implementation team. UNHCR is overly reliant on external consultants, while UNFPA is still in the process of recruiting for some key positions in its implementation team;
- The United Nations Joint Staff Pension Fund still needs to obtain approval of its Pension Board to continue applying the Financial Regulations and Rules "mutatis mutandis" to its accounting and financial reporting process in a manner that allows it to be IPSAS-compliant by 2012. The Board has identified a number of risks that need to be mitigated if the Fund is to meet its deadline of 1 January 2012.

For several entities, even if IPSAS-compliant financial statements are delivered by 2012, it is highly unlikely that the intended benefits of IPSAS adoption will be realized without significant further delay owing to the absence of appropriate benefits realization strategies and change management processes at most entities.

Recommendations

In the light of the key findings above, the Board has made detailed recommendations in the main body of this report. In summary the main recommendations are:

(a) **That the United Nations and peacekeeping operations:**

- **Fully examine all of the potential interdependencies, risks, costs and benefits of a phased implementation of Umoja and IPSAS**
- **Include contingency plans, should the phased implementation of Umoja prove impossible or fail**
- **Complete a practical and detailed implementation plan for the United Nations and peacekeeping operations as soon as possible after a decision has been made on the Umoja implementation strategy, setting out how and when accruals accounting data will be collected, cleansed and migrated to Umoja. The overarching plan should be underpinned by supporting plans at the operational level to provide a sharp focus for the efforts of departments, offices away from Headquarters and missions**

- **Develop, as a matter of urgency, an effective risk framework for IPSAS implementation.**

(b) **That all entities that have not already done so, including the United Nations and peacekeeping operations:**

- **Prepare model financial statements and produce clear plans for a "dry run" set of accounts with real accounting data, factoring in sufficient time for review by the Board**
- **Establish a fully resourced and expert IPSAS implementation team**
- **Establish a clear plan for data collection, cleansing and migration for IPSAS implementation, communicate requirements to relevant staff, and urgently commence with the exercise**
- **Establish an IPSAS benefits realization plan and organization-wide change management programme for IPSAS, including a comprehensive communications plan to set out the changes and benefits that IPSAS will bring, and how senior management in every department and office must take ownership and drive the delivery of the intended benefits.**

Table
Progress towards IPSAS implementation

Main criteria	*United Nations (2014)*	*Peacekeeping operations (mid-2013)*	*UNDP (2012)*	*UNFPA (2012)*	*UNOPS (2012)*	*UNICEF (2012)*	*UNHCR (2012)*	*UNRWA (2012)*
Board's assessment of achieving IPSAS implementation	High risk	High risk	Low risk	Medium risk	Medium-high risk	Medium risk	Medium risk	Medium risk
Entity is on track against key milestones in implementation plan	No detailed implementation plan	No detailed implementation plan	Yes	Yes	Partially; some slippage against plans	Yes	Partially; some slippage against plans	Partially; some slippage against plans
A fit for purpose enterprise resource management system is in place	No. Umoja is under development but behind schedule.	No. Umoja is under development but behind schedule.	Yes	Yes	Yes	Partially	Yes	Partially
Plans for gathering, cleansing and migrating accounting data on track	Work has only started.	Work has only started.	In progress and ongoing	In progress and ongoing	In progress and ongoing	In progress and ongoing	In progress and ongoing	Yes
Model draft financial statements have been prepared and shared with the Board	No	No	Yes	Yes	No	No	No	No
There are clear plans for establishing opening balances	Partially	Partially	Yes	Yes	Partially	Partially	No	No
Planned for a dry run using real accounting data	Partially	Partially	Yes	Yes	Partially	Partially	Yes, but timetable is tight	Yes
An effective benefits realization plan has been established	No	No	No	No	No	Partially	No	No
An effective business change management programme has been established	No	No	Yes	Partially	Partially	Yes	Partially	Partially

		Page
I.	Background	10
II.	Managing the benefits from IPSAS adoption	11
III.	Findings and recommendations on the United Nations and peacekeeping operations	16
IV.	Findings and recommendations for the United Nations funds and programmes	23
V.	Acknowledgement	32
Annexes		
I.	United Nations system organizations IPSAS implementation targets	34
II.	Budget for IPSAS implementation at the United Nations March 2011	36
III.	Examples of the accounting data required to support IPSAS-compliant financial statements	37

I. Background

1. The International Public Sector Accounting Standards (IPSAS) are accruals-based standards, written specifically for the public sector and international organizations. They are issued by the International Public Sector Accounting Standards Board, which seeks to promote transparency and accountability in the public sector. They are far more precise and detailed than the United Nations system accounting standards, and leave far less scope for inconsistent interpretation.

2. Accruals accounting means that an organization recognizes costs when they are incurred, and income when it is earned, rather than waiting until payment is made or received. IPSAS also requires details of the value, the volume and the location of an organization's assets (such as property, equipment, vehicles, food stores, medicine) and liabilities (such as pensions, staff-related liabilities, debts to suppliers, and commitments for funding), which the United Nations organizations have never captured before. Thus IPSAS is really about organizations having a much better understanding, and a more accurate picture, of its costs, income, assets and liabilities. IPSAS will provide greater managerial control over assets and liabilities, and, more importantly, will provide better information to drive cost-effective decision-making, secure better value for money and maintain long-term financial sustainability.

3. In November 2005, the High-level Committee on Management of the United Nations System Chief Executives Board for Coordination (CEB) made the landmark recommendation that United Nations system organizations move from the internally developed United Nations System Accounting Standards (UNSAS) and adopt IPSAS for the presentation of the organizations' financial statements; in essence, that the organizations adopt full accruals accounting. In 2006, the General Assembly, in its resolution 60/283, decided to approve the adoption of IPSAS.

4. The High-level Committee on Management recommended that all United Nations system organizations, with the exception of three early adopters,[1] adopt IPSAS effective no later than 2010. This implementation target proved difficult for a number of organizations for one or more reasons: a lack of IPSAS expertise; the absence of compliant enterprise resource planning systems; and conflicting organizational priorities. As at 30 June 2009, 11 organizations had revised their original timeline; two further revisions took place by 31 December 2009. As at 30 June 2010, two of the four organizations that had previously planned to implement IPSAS in 2011 had deferred to 2012, and one organization set to implement IPSAS in 2012 is now aiming for 2014. The latest implementation dates for United Nations system entities are set out in annex I to the present report.

5. The Board, in its report on peacekeeping operations for the year ended 30 June 2010 (A/65/5, vol. II), and its concise summary of principal findings issued in July 2010 (A/65/169), continued to highlight concerns with the progress being achieved, the deferral of the dates for IPSAS implementation and, in particular, the continuing problems administrations faced in accurately accounting for assets across global operations and the associated risks of qualified accounts post-IPSAS implementation.

[1] The three early adopters were the World Food Programme, the International Civil Aviation Organization and the World Health Organization. The World Food Programme successfully adopted IPSAS in 2008.

Mandate, scope and methodology

6. Against this background, the Advisory Committee on Administrative and Budgetary Questions recommended in its report issued in October 2010 (A/65/498) that the Board prepare an annual report on progress towards IPSAS implementation. Building on its previous work and ongoing engagement with United Nations entities on IPSAS matters, the Board examined progress towards IPSAS implementation across its portfolio focusing on whether the entities concerned:

- Are on track to implement IPSAS as planned;
- Have established appropriate governance and implementation arrangements and are identifying and managing the risks to successful implementation;
- Are actively managing the business transformation required to secure IPSAS-compliant processes and deliver the intended benefits.

7. There are a number of critical risks to achieving IPSAS implementation on time and to realizing the benefits envisaged by the General Assembly when it took the decision to adopt IPSAS. The Administrations have, themselves, recognized many of these risks, but the purpose of this report is to provide the Board's independent perspective on these matters, as requested by the General Assembly.

8. The Board coordinated its work where appropriate with the Office of Internal Oversight Services and other internal audit services. The Board also took account of the 2010 report of the Joint Inspection Unit entitled "Preparedness of United Nations system organizations for the International Public Sector Accounting Standards" (JIU/REP/2010/6). That report found that many United Nations organizations had underestimated the concerted efforts and resources that would be required and had failed to undertake initial preparedness and risk assessments. The review also emphasized that successful transition to IPSAS hinges on strong senior management support and engagement, dedicated intra-departmental task forces and the adoption of a project management approach, and went on to recommend the implementation of 16 best practices.

9. This report by contrast provides, for the entities reported on, a concise summary of the current status of progress, the key risks to the successful delivery of the full benefits of IPSAS, and the actions required to address these risks. It addresses matters that, in the view of the Board, should be brought to the attention of the General Assembly. The Board's observations and conclusions were discussed with the respective administrations, whose views have been appropriately reflected in this report.

II. Managing the benefits from IPSAS adoption

10. This section of the report considers the benefits that the adoption of IPSAS will confer on the entities involved, and how the realization of these benefits is being managed, including whether the associated business change management disciplines are in place or being established. It also looks at the realization of the benefits from the harmonization and comparability of accounting policies and business processes, and the impact of more timely information that will stem from annual reporting. At all times the Board's focus was on the entities contained within its portfolio and set out in the scope.

Benefits realization and change management

11. The General Assembly originally envisaged (see A/60/846/Add.3) that the benefits of IPSAS adoption were expected to include:

- Improved internal control and transparency of assets and liabilities generally
- The alignment of United Nations accounting with best accounting practices through the application of credible, independent accounting standards on a full accruals basis
- More comprehensive information on costs to better support results-based management
- Improvements in the accuracy and completeness of non-expendable equipment records
- Improved consistency and comparability of financial statements.

12. The Board is aware that the Administration made a presentation at an informal session of the Advisory Committee on Administrative and Budgetary Questions in May 2011 on the importance of managing benefits realization and the potential risks for their non-realization, both within the United Nations Secretariat and across the United Nations system.

13. The new accruals-based information on, for example, assets, inventories, investments and future liabilities will provide the bedrock for more informed decision-making in all United Nations organizations. It is therefore important that, as this information is gathered, it is given to operational managers and staff who understand and can interpret accrual-based management information, and who are empowered to think differently about, and are held accountable for, using scarce resources more cost-effectively. For these reasons, the delivery of IPSAS-compliant financial statements is only one, albeit important, milestone towards realizing the full benefits. For example, new information of the value, the cost and the useful lives of all property assets will enable entities to develop integrated property asset strategies in a way that has previously not been possible.

14. The Board recognizes that delivery of the full benefits from IPSAS adoption for financial reporting purposes and accrual accounting for management purposes will not be delivered immediately but will come through careful management, over time. Nevertheless, work towards realizing the benefits from this major change programme must start now to avoid excessive delay in their delivery. The Board is concerned that at all of the entities examined:

- The intended benefits of IPSAS adoption are not comprehensively collated in any single document, including the high-level IPSAS project plan; and there is neither an action plan for benefits delivery, nor any benefits-tracking arrangements. In essence there is no benefits realization plan for IPSAS adoption across the United Nations system organizations;
- There is little evidence that operational areas understand the new information that will be available to them, or are considering and preparing for how they will use it to improve the cost-effectiveness of their operations and deliver other tangible benefits;

- It is unclear who has accountability for delivering the benefits from IPSAS. Operational areas have not signed up to delivery of tangible and quantifiable benefits attributable to their area of the business and cannot say how the benefits will be achieved or measured.

15. **The Board recommends that the United Nations, its peacekeeping operations, and its funds and programmes: (a) clearly identify the objectives of the IPSAS project and link them to the benefits for the United Nations; (b) require operational areas to do the same for their own implementation plans; (c) develop a methodology to track the benefits from IPSAS adoption; and (d) communicate regularly on progress towards benefit realization to senior management, the Management Committee, the Advisory Committee on Administrative and Budgetary Questions and the General Assembly, as appropriate for the entity in question.**

Business change management

16. IPSAS implementation is a major business change programme. It is already impacting on staff, management and those responsible for governance and will require major cultural change if the United Nations, its peacekeeping operations, and its funds and programmes are to achieve the transition to IPSAS and reap the full benefits over time.

17. It is vital that all staff understand the impact of the new reporting regime on their day-to-day activities. Without sufficient resources being dedicated to training and change management, there is a real risk that IPSAS will not be understood and that the intended benefits will not be realized. The Board has seen little evidence of the deployment of the change management resources and methodologies needed to support IPSAS implementation and realize its intended benefits.

18. There is a risk that staff will fail to buy-in to the IPSAS project if the benefits and changes that IPSAS adoption will bring are not effectively communicated and if staff are not engaged more actively in both implementation and working towards benefits realization. In particular, the Board has seen no evidence of a communication strategy and vision of what needs to be achieved and how to do it, in particular:

- How the new information and the active management of balance sheets and cash flows will support improved accountability and the delivery of more cost-effective ways of working
- The role that United Nations finance functions will play in improving organizational performance, providing sophisticated information for decision-making, and acting as a centre of excellence in financial management for the United Nations system as a whole
- The training needed for policymakers and operational managers in the new information and how it can be used to enhance, for example, performance measurement, activity costing and investment appraisal.

19. At the United Nations, while online IPSAS awareness and basic conceptual training has been provided to over 2,000 staff, the training has been conducted on a voluntary basis and has not been managed in a tracked or targeted fashion thus far. The Administration informed the Board that its next phase of more detailed training

will be targeted at individuals who will be directly impacted by IPSAS implementation. The Board notes that all IPSAS training should emphasize the benefits of accruals accounting and how it might improve decision-making and business performance. The Board also notes that a "change manager" was engaged in April 2011, and considers that this role should incorporate developing the United Nations communications strategy for the roll out of IPSAS across the Organization. The Board also considers that effective change management will also require effective engagement, support and leadership from senior management across the United Nations.

20. At the United Nations funds and programmes, there is little evidence of the change management resources and activities needed to support IPSAS, such as staff training activities. There is also a lack of emphasis on the significant cultural and behavioural changes required to realize benefits. There is a real risk that IPSAS will not be understood and that its benefits will be lost.

21. **The Board recommends that the United Nations Management Committee and senior management within funds and programmes, establish, where absent, an IPSAS benefits realization plan and organization-wide change management programme for IPSAS, including a comprehensive communications plan to set out the changes and benefits that IPSAS will bring, and how senior management in every department and office must take ownership and drive the delivery of the intended benefits.**

22. **The Board also recommends that all senior managers within the United Nations and its funds and programmes should, as a minimum, complete IPSAS-awareness training that emphasizes the benefits of accruals accounting and how it might improve decision-making and business performance.**

Harmonization and standardization of business practices

23. IPSAS adoption is consistent with the shared aim of the United Nations system to increase its effectiveness by promoting harmonized business practices. IPSAS was agreed as the desired United Nations system standard because it has been developed through a rigorous independent process by international financial accounting experts, conferring credibility and comparability on the financial statements. This is vitally important given the United Nations entities' reliance on funding from Member States at a time of fiscal constraint. Inconsistent interpretation on major issues between United Nations entities could lead to questions as to the value of IPSAS over any other standard, including UNSAS, hence the High-level Committee for Management's understandable desire for harmonization.

24. There is a significant risk to the credibility of United Nations financial reporting and the IPSAS adoption project within the United Nations system as a whole if organizations with essentially similar business activities or administrative arrangements apply differing interpretations of the same IPSAS. There is general agreement by United Nations organizations that consistency in interpretation and application should apply when the business activities, or the administrative arrangements covered by specific IPSAS, are the same or similar.

25. In 2010 the United Nations systemwide IPSAS Task Force commissioned a survey to determine the status of the level of "diversity" between United Nations

system organizations as at December 2010. The survey indicated that where accounting policies had been agreed and approved by the Task Force there was a high level of consistent adoption, or clear reasons for non-applicability in a minority of cases, indicating a good degree of harmonization. Where the Task Force had only acknowledged guidance on the interpretation of IPSAS standards there was a wider level of variance in the level of deemed applicability or differences in interpretation. This reflects both the options available under IPSAS and disagreements on how they are to be applied and also differing levels of preparedness where some entities have established a firm position and others are still examining options. There are seven policy areas of particular concern where there are significant differences in approach, and where further dialogue between entities, and between entities and external auditors, is required and planned for mid-2011, including:

- Revenue recognition of non-exchange transactions, such as voluntary contributions, multi-year funding agreements, and goods and services in kind
- The accounting treatment for a range of employee benefits including, for example, after-service health insurance, annual leave, sick leave, death grants, education grants
- Control over project assets, where organizations have differing views on whether assets purchased as part of a project should be recognized as assets of the organization and included on their balance sheets, or should be expensed at the point of purchase because the organization has no control, and derives no benefit from, the asset
- The treatment of donated rights to use, where there are differing views on whether control and use of the asset in question requires it to be treated as an asset of the organization.

26. The Board supports the need for consistency in interpretation in the application of IPSAS as mandated by the High-level Committee for Management. Though it is clearly important for similarly placed United Nations organizations to embrace similar, if not identical, accounting treatments and policies to obtain the benefits of comparability, the pursuit of a harmonized approach must not compromise an entity's ability to deliver IPSAS-compliant financial statements and true and fair reporting. It is the responsibility of each entity's management to determine the most appropriate interpretation and application for that entity. Crucially, Member States should have the fullest possible understanding of the financial position of each individual entity.

27. **The Board recommends that, conscious of the need for each entity to apply IPSAS-compliant accounting policies to fit the entity's specific circumstance and activities, the IPSAS Task Force establish in each case the reasons for any differences in accounting policy treatments with a view to achieving greater consistency.**

28. The Board, in its 2010 concise summary of principal findings (A/65/169), noted that there were inconsistencies in business procedures across United Nations organizations that were entrenched or unchallenged by the financial regulations and rules in each entity. These inconsistencies limit the comparability of the financial statements, and the Board commented that IPSAS implementation presented an opportunity to improve consistency.

29. Work to align the Financial Regulations and Rules of United Nations system entities commenced in 2006, but had still not been completed at the date of the writing of this report. The Board recognizes that the autonomous nature of the funds and programmes may result in genuine differences in business processes and therefore the rules and regulations. In addition, the different timelines being followed for IPSAS implementation, and the necessary focus now on implementation, rather than harmonization, of financial rules and regulations means there is unlikely to be harmonization in the near future.

30. Even if the regulations and rules are aligned, unless they are also strengthened and made more precise, there will remain an inherent risk that the United Nations system will not achieve its objective of harmonized business processes. The Board will continue to consider the issue of harmonization of financial rules and regulations, business processes and the presentation of financial statements in its future reports. The Board considers that the administrations must keep the matter of harmonization under review.

Annual accounts and reporting

31. As required under IPSAS, United Nations entities will be reporting and producing financial statements on an annual basis rather than biennially. It is important that the annual financial statements are also audited so that they are credible and can be relied upon, a view which is supported by both the United Nations Panel of External Auditors and the IPSAS Task Force. This will, in turn, provide those charged with governance with more timely information of the financial position and performance of United Nations entities.

32. There will be implications from annual reporting, including the extent to which administrations used to biennial reporting are ready for annual accounts production; and how the General Assembly will manage the increased number and frequency of accounts and associated external audit reports, in particular the impact on the schedule of work of the Advisory Committee on Administrative and Budgetary Questions and the Fifth Committee.

33. The United Nations Administration is in discussion with the various stakeholders, including the Board, on potential scenarios, options and solutions that might be presented to the Advisory Committee on Administrative and Budgetary Questions for their consideration. Given that the shift to annual reporting will have an impact from 2012 onwards, there is a pressing need for the United Nations Administration to resolve this matter.

III. Findings and recommendations on the United Nations and peacekeeping operations

A. Progress against implementation deadline

Deadline for IPSAS implementation in the United Nations and peacekeeping operations

34. As at 30 June 2009, the United Nations had revised its original 2012 IPSAS implementation deadline (including for peacekeeping operations) from 2012 to 2014. The key dates are as follows:

- The first full year of IPSAS adoption on peacekeeping will be the financial year ended 30 June 2014, which means that the Administration will need to be ready in all practical aspects by 1 July 2013
- The first full year of IPSAS adoption for the United Nations will be the financial year ended 31 December 2014, which means that the Administration will need to be ready by 1 January 2014.

35. The Administration explained that the decision to delay was taken in order to coordinate IPSAS implementation with Umoja readiness because the existing resource and asset management systems are unable to produce the accounting data needed to produce IPSAS-compliant financial statements without significant and costly enhancement or manual interventions. In late 2010 it became clear that the timetable for Umoja had slipped and in March 2011 the United Nations Management Committee was informed that Umoja was at least 10.5 months behind its target delivery date (December 2014); it will therefore not be fully deployed until 2015, and is therefore unable to support IPSAS implementation as planned.

36. In March 2011, a joint working group, chaired by a representative of the Department of Field Services, was established to facilitate improved coordination between the two projects and support the Umoja Project Director in developing and presenting an IPSAS-supportive Umoja strategy and timeline to the Umoja Steering Committee. At the time of the Board's examination, the implementation of Umoja was being reassessed to see whether it could be refocused on the delivery of the elements needed to support IPSAS implementation on target for 2014. A decision on this was expected between June and August 2011, at which point there will be less than 24 months to be ready for peacekeeping (1 July 2013). The Board also notes that the Umoja Project Director resigned in June 2011, and at the time of writing of this report it was unclear to the Board what the full implications of this are for Umoja, and therefore IPSAS delivery.

37. While there is a clear logic in prioritizing the parts of Umoja that support IPSAS, other elements of Umoja will by necessity be delayed if this is done. This could create risks to business transformation in other priority areas; and also presents risks to the momentum and budgets for Umoja, as staff could become exhausted and funding could be depleted, potentially delaying, or even reducing, the full delivery of the intended benefits from Umoja. The potential interdependencies, risks and benefits need to be thoroughly considered, and set out to enable informed decision-making. The Board is also concerned that, should the phased implementation of Umoja prove impossible, or only partially possible, there is currently no agreed contingency plan. The Board considers that any further deferral of the date of IPSAS implementation would be damaging to the reputation of the United Nations and would put the successful adoption of IPSAS at risk. It is therefore vital that the United Nations develop a pragmatic and viable contingency plan to achieve the 2014 implementation target without Umoja.

38. **The Board recommends that the Administration fully examine all of the potential interdependencies, risks, costs and benefits of a phased implementation of Umoja and IPSAS.**

39. **The Board also recommends that the Administration finalize and agree contingency plans, should the phased implementation of Umoja prove impossible or fail.**

40. The Administration stated that it was mindful of the need to manage the realization of the benefits of both projects, and informed the Board that the Management Committee was informed in late June that the Umoja project cannot be fully rephased to support IPSAS implementation. The Administration has, therefore, started developing contingency plans to mitigate the risks arising from potential delays in the deployment of Umoja. The intention is that the contingency plans, which will include some rephasing of Umoja, limited modifications to current functional systems and some manual workarounds will be periodically reviewed by the Administration to adapt to the progress of both projects. The Board has yet to see any plans and stresses that any manual workarounds can only be temporary stopgaps for a limited period prior to the implementation of a fully functional enterprise resource management system.

Implementation plan

41. The Administration informed the Board that the IPSAS project has operated on the basis of a high-level implementation plan focusing on accounting policy gaps, the development of training materials and the design work needed for Umoja. Up to 2010 other work had included progressive implementation of IPSAS requirements, including, for example, the recognition of and detailed disclosure on liabilities relating to after-service health insurance; rationalization of the construction in progress accounting for the capital master plan; and disclosures on in kind contributions and contingent liabilities. These developments have started to help pave the way for all parts of the United Nations to embrace the changes IPSAS implementation will bring about, but they are only a start.

42. In late 2010 the Administration initiated production of a more detailed implementation plan than had previously been available. This will include templates for detailed planning in operational areas (missions, departments and offices) with far more focus on the practical and logistical challenges in implementing new business processes and collecting and preparing the raw accounting data needed for IPSAS implementation. The United Nations has also conducted a recent survey to assess office and mission readiness for IPSAS implementation and to identify the scale of work to be performed. At the time of this report the detailed implementation plan remained a work in progress with a target for approval later in 2011.

43. The implementation plan has to be finalized in consultation with missions and offices away from headquarters, and the Board notes that this was discussed at the Chief Finance Officers' workshop in June 2011, with a view to finalizing site-specific plans shortly thereafter. The increased emphasis on addressing practical implementation is welcomed by the Board. Without a clear overarching implementation plan, it remains difficult for operational areas to engage effectively with IPSAS adoption; and without clarity on the decisions regarding Umoja and a detailed implementation plan, the Board cannot provide any firm assurance that the United Nations is on track to deliver IPSAS adoption by 2014. Development of a detailed implementation plan is now a critical path task and cannot be delayed. Some of the key tasks that must be clearly set out in the implementation plan are set out below:

(a) **Preparation of accounting data**: There is a huge amount of new data that needs to be captured across the United Nations global operations in order to achieve IPSAS compliance. For example, data on the value, the volume and the

location of assets, a task that is particularly acute for peacekeeping, where the majority of United Nations assets are held. There is also the significant task of migrating "legacy" accounting data from the numerous existing systems into the new Umoja system. At the time of the Board's review, the bulk of this systematic data collection and cleansing had only recently been started, and the Administration could not provide the Board with a clear plan for cleansing and migrating data from the "legacy" systems into Umoja and making this available for audit. The scale of this critical task cannot be underestimated, and annex II illustrates the range of data that needs to be prepared and the challenges involved. The Board notes, and welcomes, that the Office of Internal Oversight Services (OIOS) has been developing work programmes to support the Administration in preparing accounting data and reinforcing compliance by operational areas. The Board will be coordinating closely with OIOS so that this work can help provide the assurance required by the Board;

(b) **Development of draft financial statements**: Developing a "dry run" model set of accounts using real accounting data allows the United Nations to test its readiness to produce IPSAS-compliant accounts while enabling the Board to identify potential weaknesses and provide advice in advance of IPSAS implementation. The United Nations IPSAS Implementation Team has prepared a model IPSAS account, but because of unresolved issues on accounting policies, it has not yet been provided to the Board. The implementation team is also aware of the importance of having draft financial statements populated with actual data for assessment by the Board, but is not confident that it has the resources to prepare full scope "dry run" accounts. Without a "dry run" with real data it is unlikely that an organization as complex as the United Nations will be able to achieve financial statements of sufficiently high quality to withstand audit within the planned implementation time frames;

(c) **Audit of opening balances**: The development of model financial statements will be supported by an exercise to establish opening balances for assets, liabilities and reserves for the first year of adoption. This is in effect the starting point under full accruals accounting from which the opening financial position is established. The Board notes that the IPSAS Implementation Team is anticipating that opening balances will be prepared on a "progressive basis", fund by fund, and made available to auditors on that basis. As with the uncertainty over the collection of key accounting data, the Board is concerned that there is a lack of clarity on how opening balances and an opening balance sheet will be developed through this progressive approach and the time frames for this.

44. **The Board recommends that the Administration prepare a complete, practical and detailed implementation plan for the United Nations and peacekeeping operations as soon as possible after a decision has been made on the Umoja implementation strategy.**

45. **The Board also recommends that the Administration's implementation plan:**

(a) **be underpinned by supporting plans at the operational level to provide a sharp focus for the efforts of departments, offices away from headquarters and missions;**

(b) set out how and when accruals accounting data on non-expendable property, leases, legal obligations, guarantees, consumable inventories, contracts and locally recruited staff will be collected, cleansed and migrated to Umoja and made available for audit;

(c) include clear plans to benchmark the United Nations financial statements against an IPSAS compliant set to establish the necessary action and revisions required to meet the implementation timetable; and produce a "dry run" set of accounts with real accounting data for review by the Board;

(d) include clear plans for the creation of opening balances and balance sheets that should be shared with the Board as soon as possible. The plan should be risk based, focusing on the preparation of opening balances by the most material offices first, and factor in sufficient time for the Board to conduct an audit of the opening balance sheet as soon as is practicably possible and certainly no later than three months before the end of the first live year of IPSAS adoption.

46. The Administration informed the Board that, owing to the tight timetable, it might not be possible to produce complete "dry run" accounts, but that it intended to carry out dry runs on the most material and high risk funds for United Nations and peacekeeping operations. The Board will follow up on the planning for dry run audits as a matter of urgency during 2011.

B. Governance and implementation arrangements

47. The United Nations Management Committee, chaired by the Deputy Secretary-General, has overall responsibility and oversight of the IPSAS and Umoja business transformation projects. The United Nations IPSAS project is overseen by the IPSAS Steering Committee, which is chaired by the United Nations Controller. The Umoja Steering Committee is chaired by the Under-Secretary-General for Management. Prior to December 2010, the two steering committees reported periodically to the Management Committee. The governance arrangements have been strengthened more recently with the requirement for both the IPSAS and Umoja steering committees to report quarterly to the Management Committee.

48. Given the scale and technical aspects involved in each, it is understandable and appropriate that separate steering committees have been established for IPSAS and Umoja implementation. It is clear that the interdependencies between the two are very strong, and both are working towards similar goals in more than one area; for example, more effective policies and processes for financial management. This interdependency has been further highlighted by the impact of delays to Umoja and the establishment of the new joint IPSAS and Umoja working group.

49. The Board considers the increased joint working and coordination between the project teams a positive development. Given the challenges to delivering the benefits from IPSAS, which are in turn dependent on revised business processes and a fully functional enterprise resource planning system, the Board would encourage the Administration to consider other areas in which joint working can be delivered, especially as operational areas are increasingly drawn into implementation and demands are placed on them by both projects. In the meantime, the Board notes that

the working group does not have formal terms of reference and it is unclear how the decisions that it takes will be approved and enforced.

50. At the United Nations the business change activities for Umoja and IPSAS could potentially be combined to bring benefits in terms of costs (for communications, training, staff time) and effectiveness. The change management messages would be more powerfully delivered as a joint message, and would more effectively use senior management time. They would also help change the perception that IPSAS is a technical financial initiative and start to ground it in people's minds as something that can have real impact for them.

51. To realize the full benefits from new processes and information from both IPSAS and Umoja, there needs to be a clear and effective accountability and risk management framework for the organization as a whole; and implicit in this observation is the need to align both the appropriate accountability and authority for those managers delivering the services of the United Nations. These are necessary precursors for benefits realization, which must be integrated within an overall change programme. Otherwise, management will not be empowered or accountable for using the new information to improve the cost effectiveness of their activities and the full benefits will not be realized. The Board is aware of various initiatives to improve accountability and risk management in the United Nations, and this is an issue the Board will be considering further in its future reports.

52. **The Board recommends that the Administration assess the feasibility of combining the business change activities for Umoja and IPSAS.**

53. **The Board recommends that the Administration include the new and important joint working group in its formal governance structure and establish clear terms of reference that clarify how its decisions will be approved and enforced.**

Implementation team

54. It is important that for any major business transformation project there be a dedicated, well resourced and capable project implementation team. The United Nations established the IPSAS Implementation Project Team in 2007. It has an agreed complement of 18 staff, but at the time of our review had three vacancies, and has operated for over 12 months with a reduced team. Key posts have been left vacant, including a change manager to coordinate the IPSAS project with the delivery of Umoja business processes and to manage other aspects of this business transformation, including training. The Administration informed the Board that it had deliberately left these posts vacant so as to protect its budget for the implementation phase. The Board is of the view that the vacancies have inevitably contributed to a delay in completing a detailed implementation plan. The Board was informed that the project team will be up to full strength by December 2011, including the recruitment of a "change manager".

55. **The Board recommends that the Administration establish an IPSAS implementation team based on a reassessment of the resources, skills and experience required, in the light of the revised implementation plan, the scale of the tasks, and the change management challenges.**

56. The IPSAS Implementation Team has developed an extensive series of IPSAS accounting policy papers, and the Board is engaged in advising on these. On current

projections, the approved accounting policy framework will not be completed until March 2012. The roll out of most of the IPSAS policies to the operational units will be done through Umoja and will, for the most part, be blended with the Umoja implementation. Beyond the current concerns over the implementation strategy and delays to Umoja, the Board considers there is a risk that this timetable will leave insufficient time for operational areas to be ready to implement the policies and associated processes correctly and consistently. Given the scale of peacekeeping operations in particular, this is a serious risk to achieving compliant financial statements in the first year of implementation.

57. **The Board recommends that in developing the IPSAS implementation plan, the Administration factor in adequate time and resources for an appropriate level of consultation with the Board prior to approval to identify any potential risks or problems arising from its adoption.**

58. It is recognized good practice on any major project to establish a core group responsible for handling the considerable project management disciplines required for successful delivery, progress tracking and reporting, and for creating a common project management approach across the organization. The Board noted that the United Nations IPSAS Implementation Team is creating a Project Management Office for this purpose, which it envisages will help both reduce the administrative burden in missions and offices, and raise the visibility on progress at all levels within the United Nations.

IPSAS budget

59. The overall indicative budget approved by the General Assembly for IPSAS adoption in 2006 is $23 million (see annex II). This excludes the considerable but unquantifiable costs that will be involved as operational areas are increasingly drawn into implementation. As at the end of February 2011, the Administration had spent some $4.7 million between 2006 and 2011, with $6.1 million still available to the end of the current biennium.

60. The budget proposed for 2012-2013 has been substantially reduced as part of the Secretary-General's required cost reduction across the United Nations, although the Administration informed the Board that the eventual total budget for IPSAS adoption would remain at the $23 million initially approved by the General Assembly. The Board considers that this may be unhelpful, given the challenges to IPSAS implementation, and may prove problematic if in the longer term this delays the implementation, thereby increasing costs overall, and the delivery of the benefits (the "return"). The Board noted that there will be a need to reassess the adequacy of the IPSAS budget and to align it with the detailed implementation strategy.

61. The Board also noted that within the overall $23 million budget (see annex II) there is an allocation set aside for $7.5 million for the use of consultants, $5.7 million for general temporary assistants and $5.2 million for contractual services, travel and other expenses. This compares with only $4.6 million for established permanent posts. This may be an indication that the IPSAS Implementation Team has been smaller than desired, and therefore a significant amount of short-term, external support may be required. The Board is concerned that the approach of using consultants is balanced against the need to develop sustainable internal financial management capacity and capability.

62. **The Board recommends that, in developing the new implementation strategy, the Administration reassess the IPSAS budget to ensure that the budget available is commensurate with the updated plans for implementing IPSAS and that adequate resources are available to support the new strategy to meet the timetable for first financial statement adoption and beyond.**

Risk assessment and management

63. The Board is concerned that no formal and structured approach to risk management, including a risk register, had been established for the IPSAS implementation project at the time of the review. For this major business transformation project, the Board would have expected, from the outset, to see the main risks to the project identified, prioritized in order of severity, clearly assigned to owners with the authority to manage them, and with clear mitigating actions and regular risk reporting. The March 2011 presentations to the Management Committee on the status of the IPSAS and Umoja projects did summarize the key risks to each project, with particular emphasis on establishing reliable opening balances for assets and liabilities, producing compliant financial statements and obtaining external audit acceptance for accounting policies. There was, however, no assessment of the probability of these risks occurring or their likely impact, nor any detailed plans for how these risks will be mitigated beyond some higher level considerations.

64. **The Administration agreed with the Board's recommendation that the joint IPSAS/Umoja working group, as a matter of urgency, develop a risk framework for IPSAS implementation, identifying the main risks to implementation, setting how the risks will be mitigated (including establishing a contingency budget if appropriate), and assigning ownership and accountability for their management.**

65. The Administration commented that the United Nations IPSAS implementation team had developed and presented a risk register to the IPSAS Steering Committee in June 2011. Work has now started on developing mitigation strategies and assigning clear ownership and accountability for each risk.

Revision of the United Nations Financial Rules and Regulations

66. The IPSAS Implementation Team is currently working on proposed revisions to the Financial Regulations and Rules of the United Nations to reflect the adoption of accruals accounting and IPSAS. This work is expected to be completed for approval by the General Assembly in the fall of 2011. The Board has not seen the proposed amendments but is aware of the Administration's intention to provide them to the Board to confirm the consistency of the new rules and regulations with the fundamentals of accruals accounting prior to approval.

IV. Findings and recommendations for the United Nations funds and programmes

Overall summary

67. This section of the report covers seven United Nations funds and programmes, including the United Nations Joint Staff Pension Fund, all of which have a planned

IPSAS adoption date of 2012. While conscious that the entities are at different stages of their planned implementation schedules, the Board's view is that implementation of IPSAS by 1 January 2012 is possible for these entities, but that there are key tasks yet to be completed in some entities and significant risks that need to be mitigated if IPSAS is to be implemented on time. With minimal time left to the target date, these entities cannot afford slippages.

68. Even if IPSAS-compliant financial statements are delivered by 2012, it is unlikely that the intended benefits of IPSAS adoption will be realized without a significant further delay owing to the absence of appropriate benefits realization strategies and implementation plans at most entities.

69. The Board has provided each of the entities with detailed feedback in observation memorandums and management letters and will continue to report in detail at the entity level. In this report, the Board has summarized in table 1 important elements of the IPSAS implementation plans to provide an overview of the entities' progress as at the date of its review.

Table 1
Progress against implementation targets

Main criteria	*UNDP*	*UNFPA*	*UNOPS*	*UNICEF*	*UNHCR*	*UNRWA*
Risk to 2012 IPSAS implementation	Low risk	Medium risk	Medium-high risk	Medium risk	Medium risk	Medium risk
A comprehensive implementation plan is in place	Yes	Yes	Yes	Yes	Yes	Yes
The plan identifies the appropriate milestones	Yes	Partially	Yes	Yes	Yes	Yes
The entity is on track against the key milestones	Yes	Yes	Partially; some slippage against plans	Yes	Partially; some slippage against plans	Partially; some slippage against plans
A fit for purpose enterprise resource management system is in place	Yes	Yes	Yes	Partially; user acceptance testing has been launched and will be complete at end August 2011	Yes	Partially; relies on a legacy system that is partially compliant and may not be sustainable in the long term
Plans for gathering, cleansing and migrating accounting data on track	In progress and ongoing	In progress and ongoing	In progress and ongoing	In progress and ongoing	In progress and ongoing	Yes
Model draft financial statements have been prepared and shared with the Board	Yes	Yes	No	Yes	No	No
There are clear plans for establishing opening balances	Yes	Yes	Partially	Partially; plans not completed at time of audit	No	No; not sufficiently detailed
Planned for a "dry run" using real accounting data	Yes	Yes	Partially	Partially	Yes, but timetable is tight	Yes

Progress against implementation targets

70. The Board reviewed the progress made by funds and programmes against the milestones set out in their implementation plans and found that some entities were behind schedule. Generally, the Board noted that the entities had detailed plans, supported by milestones, and that the progress against these milestones was monitored and reported to senior management.

71. **The Board recommends that all entities that have not already done so: (a) implement adequate project monitoring controls; (b) enhance their plans to include detail on preparation of "dry run" model financial statements and opening balances; and (c) prioritize activities required on and before the go-live date against activities that could be performed after the go-live date (particularly for those entities that are behind schedule).**

Model financial statements and "dry run" accounts

72. The preparation of model financial statements and "dry run" accounts are crucial steps in implementing IPSAS. It provides the entities with an early opportunity to test their readiness to prepare IPSAS-compliant financial statements while enabling the Board to identify potential weaknesses and provide advice. Model financial statements have been prepared and presented to the Board by UNDP and UNFPA; but these did not yet contain real accounting data and need to be revised and discussed with the Board again after the completion of further accounting policy revisions at these entities. While completion of the model financial statements is included in their respective plans, the remaining entities have not yet prepared model financial statements.

73. Although most entities were planning to develop "dry run" statements prior to implementation, using real accounting data, the Board is concerned that the timetable for doing so will be compact, and any delays could leave inadequate time for review and correction. The time frames to complete biennial accounts, which will form the precursor for the preparation of opening balances, may also affect the time frames to perform a "dry run" exercise.

74. **The Board recommends that all entities that have not already done so (a) benchmark their financial statements against an IPSAS-compliant set to establish the necessary action and revisions required to meet the implementation timetable; and (b) prepare model financial statements and produce clear plans for a "dry run" set of accounts with real accounting data, factoring in sufficient time for review by the Board.**

Enterprise resource planning systems

75. The increased requirements for data on accounting transactions under IPSAS mean that the entities need more advanced enterprise resource planning systems to implement the standards. Work to establish a fit for purpose enterprise resource planning system is well advanced at most of the entities. For example, UNDP, UNOPS and UNFPA co-own a now-established enterprise resource planning system (Atlas). Whereas each of these entities is responsible for its own system's specification and configuration, UNDP has overall responsibility on behalf of all three entities. At UNDP progress on the system specification and configuration was behind schedule. UNDP, UNOPS and UNFPA need to closely monitor how the

activities of the UNDP Office of Information System and Technology are designed to meet the timelines for their respective system customizations.

76. Owing to budgetary constraints, UNRWA is planning to implement IPSAS using its current enterprise resource planning system, despite a gap study that it commissioned in 2008 that concluded that the system could only reach partial compliance and may not be sustainable in the future. UNRWA indicated that it would submit the required system changes to its supplier to determine whether the system would be able to accommodate them as soon as the policies and procedures are complete. The Board considers this a significant risk, which will need to be closely managed to avoid any delay to IPSAS implementation.

77. **The Board recommends that UNDP, UNOPS and UNFPA keep under review how the activities of the UNDP Office of Information System and Technology are designed to meet the timelines for their respective enterprise resource planning system customizations.**

78. **The Board also recommends that UNRWA keep under close review the risk of its current enterprise resource planning system being unable to comply with IPSAS and develop contingency plans, as appropriate.**

Data collection

79. Across all entities significant work remains to adequately collect, cleanse and migrate data for IPSAS implementation. The complexity of data collection is increased under IPSAS, as the entities need to consider data maintained at the field level and country offices. Annex III sets out examples of data that needs to be collected to support compliance with IPSAS standards. The Board noted that most entities had included data cleansing and migration as part of their implementation plans, although generally there were slippages on the schedules. At UNFPA the Board noted that the cleansing tasks were assigned to different business units and may need to be tracked as part of the IPSAS project to ensure alignment with the overall IPSAS project plan. The Board is concerned that without adequate plans, staff in field or country offices might not be trained and familiar with the new policies and procedures necessary for IPSAS implementation; for example, the need to accurately catalogue the volume and the value of assets.

80. **The Board recommends that all entities that have not already done so establish clear plans for data collection, cleansing and migration for IPSAS implementation and urgently commence with the exercise.**

Table 2
Governance and implementation arrangements

Main criteria	*UNDP*	*UNFPA*	*UNOPS*	*UNICEF*	*UNHCR*	*UNRWA*
The Governance arrangements are fit for purpose and involve senior management	Yes	Yes	Yes	Yes	Yes	Yes
A fully resourced and capable implementation team is in place	Yes	Partially	Partially	Yes	Partially; some reliance on external experts	Partially; no project leader or dedicated IPSAS implementation team
Up to date and adequate budget in place	Yes	Yes	Yes	Yes	Yes	Partially, but not adequate except for engaging consultants where needed
The project has a structured risk management framework	Yes	Yes	Yes	Yes	Yes	Partially
Accounting policy framework is complete	Substantially complete; one policy to be finalized	Substantially complete; one policy to be finalized	Partially; only two policies finalized	Partially; some policies still under development	Partially; not all policies finalized and approved	Partially; only two policies finalized
Field offices ready to implement the new policies/procedures	Partially; Global Shared Service Centre to manage complex country office transactions awaits host government agreement and finalization of staff recruitment	Partially	Partially	No; procedures for field offices not yet ready or rolled out	No; procedures for field offices not yet ready or rolled out	Not applicable

Main criteria	*UNDP*	*UNFPA*	*UNOPS*	*UNICEF*	*UNHCR*	*UNRWA*
The financial rules and regulations have been revised, and approved	Yes; revised financial rules and regulations finalized and awaiting approval	Yes, well advanced	Partially; further revision is in progress	Yes; financial rules and regulations finalized and awaiting approval	Partially; drafts received by Board June 2011	No

Governance of the IPSAS project

81. The Board found that the governance arrangements were fit for purpose and involved senior management at all of the entities.

Development of accounting policies

82. Development of accounting policies to comply with IPSAS is a crucial early step towards implementation. Delays are likely to result in a congested plan to address the required system configurations, revise business processes and prepare field and country offices to implement the new policies. The Board noted that, while some entities have made significant progress in terms of the finalization of accounting policies (UNDP and UNFPA, UNICEF and UNHCR), some entities (UNOPS and UNRWA) had significant amounts of work left to finalize their accounting policies. This presents major risks as the accounting policies selected have major implications for data gathering processes, training strategies and, most importantly, the customization of enterprise resource planning systems. The Board emphasizes the need for all entities to finalize their accounting policies for compliance with IPSAS and provide them to the Board for review.

83. **The Board recommends that all entities that have not already done so establish adequate strategies to mitigate the risk of a congested plan in the period leading up to 1 January 2012.**

Budget resources available for implementation

84. The Board reviewed the extent to which each entity has an adequate budget for IPSAS adoption and how performance against budget is being managed. Generally the IPSAS project teams were adequately resourced with appropriate input from relevant stakeholders and steering committees supporting the project teams. The Board noted that UNOPS and UNRWA relied predominantly on internal staff, and did not engage IPSAS specialists. However, their respective budgets and plans catered for the use of consultants to assist the internal teams. The use of internal staff in the project has certain benefits to these entities in terms of reducing costs and retaining knowledge, but entities need to manage the risk of their accounting policies and procedures being insufficiently aligned with IPSAS and of conflicting staff schedules, especially as the target date draws near. The specified IPSAS budgets in these entities may not therefore be a true reflection of the resources actually extended in implementing IPSAS because the budgets do not reflect the time spent by internal finance staff.

85. UNRWA has put on hold its plans to hire a dedicated project leader because of budgetary constraints. UNHCR will need to rely on external consultants for some tasks, but in the longer term will need appropriately qualified staff for delivering and securing the benefits from IPSAS post adoption. UNFPA is still in the process of recruiting for key positions in its implementation team, while the recruitment process for one post has been temporarily frozen owing to budget constraints. UNOPS has only one IPSAS-dedicated staff member and had not yet recruited other staff to support the implementation of IPSAS.

86. **The Board recommends that all entities which have not already done so (a) establish fully resourced and expert IPSAS implementation teams; and (b) review the adequacy of their budgets against their most up to date plans for IPSAS implementation and put in place appropriate resources accordingly.**

Table 3
Managing the delivery of the full benefits from IPSAS

Main criteria	*UNDP*	*UNFPA*	*UNOPS*	*UNICEF*	*UNHCR*	*UNRWA*
Operational areas have been fully engaged in identifying the potential benefits	Partially	Partially	Partially	Partially	Partially	Partially
An effective benefits realization plan has been established	No	No	No	Partially	No	No
Staff training	Partially	Partially	Partially	Yes; specific training strategy and plan in place; training will be conducted from August 2011	Plans are in place ready for roll out	Partially
Communication strategy	Yes	Yes	Yes	Yes	Partially	Yes
An effective business change management programme has been established	Yes	Partially	Partially	Yes	Partially	Partially

Benefits realization plans

87. Even if IPSAS-compliant financial statements are delivered by 2012, it is highly unlikely that the intended benefits of IPSAS adoption will be realized without a significant further delay, owing to the absence of appropriate benefits realization strategies and implementation plans at most entities.

88. **The Board recommends that all entities establish an IPSAS benefits realization plan and organization-wide change management programme for IPSAS, including a comprehensive communications plan to set out the changes and the benefits that IPSAS will bring, and how senior management in every department and office must take ownership and drive the delivery of the intended benefits.**

United Nations Joint Staff Pension Fund

89. The Board is aware that the United Nations Joint Staff Pension Fund is in the process of re-examining its implementation strategy. The Fund uses the Financial Regulations and Rules of the United Nations. These will be revised in 2012 at the earliest, adding an element of uncertainty to the Fund's IPSAS implementation by 2012. The Fund is seeking to obtain the approval of the Pension Board to continue applying the Financial Regulations and Rules "mutatis mutandis" to its accounting and financial reporting process in a manner that allows it to be IPSAS-complaint; and will request the Pension Board to endorse this transitional provision for approval by the General Assembly at its sixty-sixth session in 2011.

90. The Board has noted a number of other risks that the Fund will have to address, if it is to implement IPSAS by 2012. In particular, the Board has noted (a) an inadequate implementation strategy; (b) limited progress in developing accounting policies; (c) the absence of a Chief Finance Officer to lead the project, as well as a dedicated and integrated implementation team; and (d) the need to fully assess the impact of IPSAS implementation on its systems. In the light of these risks, the Board is concerned that the Fund's strategy to implement IPSAS by 2012 may be unrealistic.

91. **The Board recommends that the Fund, as a whole, (a) finalize its IPSAS implementation strategy considering the decision of the Pension Board; and (b) develop risk mitigation plans to address the identified risks.**

V. Acknowledgement

92. The Board wishes to express its appreciation for the cooperation and the assistance extended to its staff by the Management of the entities concerned and members of their staff.

(*Signed*) Amyas **Morse**
Comptroller and Auditor-General of the United Kingdom of Great Britain and Northern Ireland
Lead auditor

(*Signed*) Terence **Nombembe**
Auditor-General of the Republic of South Africa

(*Signed*) **Liu** Jiayi
Auditor-General of the People's Republic of China
Chair of the Board of Auditors

12 July 2011

Annex I

United Nations system organizations IPSAS implementation targets

Year	*No. of organizations*	*Organizations*
2014	2	United Nations (including peacekeeping operations)*[a]
		World Trade Organization
2012	10	Food and Agriculture Organization
		International Labour Organization
		United Nations Development Programme*
		United Nations University*
		United Nations Population Fund*
		United Nations High Commissioner for Refugees*
		United Nations Children's Fund*
		United Nations Office for Project Services*
		United Nations Relief and Works Agency for Palestine Refugees in the Near East*
		United Nations Joint Staff Pension Fund*[b]
		World Health Organization
		United Nations Women*[c]
2011	2	International Atomic Energy Agency
		Universal Postal Union
2010	8	International Civil Aviation Organization
		International Maritime Organization
		International Telecommunications Union
		Pan American Health Organization
		United Nations Educational, Scientific and Cultural Organization
		United Nations Industrial Development Organization
		World Intellectual Property Organization
		World Meteorological Organization

Year	*No. of organizations*	*Organizations*
2008	1	World Food Programme (in the third year post full IPSAS implementation)

* Audited by the United Nations Board of Auditors.

[a] The United Nations Office on Drugs and Crime, United Nations Environment Programme, United Nations Human Settlements Programme and the International Trade Centre (UNCTAD/WTO) are linked to the United Nations IPSAS adoption.

[b] The United Nations Joint Staff Pension Fund is tentatively planning to move its implementation of IPSAS to a period that coincides with that of the United Nations.

[c] United Nations Women shall adopt IPSAS in keeping with the schedule of the United Nations Development Programme. It is in its first year of operations (2011).

Note: The United Nations Framework on Climate Change, the United Nations Institute for Training and Research and the United Nations Convention to Combat Desertification do not report to the General Assembly but will adopt IPSAS in 2014.

Annex II

Budget for IPSAS implementation at the United Nations

March 2011

The General Assembly was informed that the estimated budget for IPSAS is $23.034 million. The budget is approved separately for each fiscal cycle under the regular budget and the support account for peacekeeping operations. The status of expenditures is reflected below:

Projections of expenditures of IPSAS adoption at the United Nations

(Thousands of United States dollars)

	*2006-2011** *Expenditures*	*2010-2011* *Balance*	*2012-2013* *Estimates***	*2014*	***IPSAS Totals***
(1) Regular budget					
Section 28B, Office of Programme Planning, Budget and Accounts					
Posts	2,271.1	541.4	1,179.7	589.9	**4,582.0**
General temporary assistance	-	656.8	657.4	328.7	**1,642.9**
Consultants	-	488.5	193.8	193.8	**876.1**
Travel of staff	118.5	93.8	37.3	50.0	**299.6**
Contractual services	16.7	583.4	583.4	583.4	**1,766.9**
Other	43.5	24.6	41.4	20.0	**129.5**
Subtotal, Section 28B, Office of Programme Planning, Budget and Accounts	2,449.8	2,388.5	2,693.0	1,765.8	**9,297.1**
					-
Section 31, Jointly Financed Activities					-
Grants and contributions	1,335.9	241.3	500.0	200.0	**2,277.2**
Total regular budget	**3,785.7**	**2,629.8**	**3,193.0**	**1,965.8**	**11,574.3**
					-
(2) Peacekeeping support account***					-
General temporary assistance	871.8	809	1,580.8	790.4	**4,051.7**
Consultants	62.4	2,582	3,351.7	650.0	**6,646.1**
Travel	20.2	62	405.4	202.7	**690.1**
Other	-	-	52.2	18.8	**71.0**
Total support account for peacekeeping operations	**954.4**	**3,452.5**	**5,390.1**	**1,661.9**	**11,458.9**
Grand total (1) and (2)	**4,740.1**	**6,082.3**	**8,583.1**	**3,627.7**	**23,033.2**

* Total expenditures as of 28 February 2011.

** These figures are high-level estimates.

*** Peacekeeping support account 2010-2011 balance includes allotment of 2010/11 and estimates of the first six months of 2011/12.

Annex III

Examples of the accounting data required to support IPSAS-compliant financial statements

Existence, ownership and valuation of fixed assets. This will be a major issue for many entities, in particular for United Nations peacekeeping operations. The United Nations needs to unequivocally establish what assets it owns, how much they are worth and how much use they can get from them. This is critical to establishing its asset base and future charges for the consumption of these assets. This will potentially require professional external asset valuations and determinations of the assets remaining useful lives of all assets catalogued.

Procurement. There are at present some 220 framework agreements and thousands of individual contracts or one-off agreements, each containing a complex set of procurement arrangements. During the process of assessing progress towards the adoption of IPSAS, the type of contract entered into will impact on the accounting for the related transactions, assets and liabilities. It will therefore be important to consider the nature of these contracts to determine if they are asset purchases, service purchases, financial leases, operating leases, or financial instruments.

Legal obligations and guarantees. Again, this is fundamental to establishing the correct accounting treatment of these obligations and guarantees much in the same way as for leases.

Preparation of non-expendable property and expendables data for conversion to IPSAS. The values and volume of this data is expected to be enormous (e.g., the Food Supply Management system provides for the procurement and the distribution of food supply for some 100,000 United Nations forces personnel in the field). The challenge will be in ensuring that capture of this data is as complete and reliable as needed to avoid material omissions or errors in the financial statements.

Information on locally recruited staff at missions. In addition to international staff for which records are kept centrally, some 10,000 personnel are recruited locally in field locations for peacekeeping, special political or other missions. At present, the information is kept on a multitude of local systems and manually consolidated into the relevant financial statements. In addition both international staff and locally recruited staff are entitled to a range of staff benefits such as repatriation grants, education grants, subsistence allowances and after-service health insurance. For IPSAS adoption information will be needed on staff leave, including accumulated outstanding leave; and staff benefit payments, in particular details of accrued benefits such as education grants, which are now available for locally recruited staff: and entitlement to any after-service benefits and the potential liabilities relating to these.

United Nations A/6

General Assembly

Distr.: General
15 July 2011
English
Original: English/Russian

Sixty-sixth session
Item 93 of the provisional agenda*
Developments in the field of information and telecommunications in the context of international security

Developments in the field of information and telecommunications in the context of international security

Report of the Secretary-General

Contents

I. Introduction ....
II. Replies received from Governments ....
Australia ....
Georgia ....
Germany ....
Greece ....
Kazakhstan ....
Netherlands ....
United States of America ....

* A/66/150.

11-41691 (E) 250711 290711

Please recycle

BEST COPY AVAILABLE

I. Introduction

1. In paragraph 3 of its resolution 65/41, the General Assembly invited all Member States, taking into account the assessments and recommendations contained in the report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,[1] to continue to inform the Secretary-General of their views and assessments on the following questions:

(a) General appreciation of the issues of information security;

(b) Efforts taken at the national level to strengthen information security and promote international cooperation in this field;

(c) The content of the concepts mentioned in paragraph 2 of the resolution;

(d) Possible measures that could be taken by the international community to strengthen information security at the global level.

2. Pursuant to that request, on 16 March 2011, a note verbale was sent to Member States inviting them to provide information on the subject. The replies received are contained in section II below. Any additional replies received will be issued as addenda to the present report.

II. Replies received from Governments

Australia

[Original: English]
[31 May 2011]

Australia welcomes the opportunity to submit this reply containing our views, pursuant to General Assembly resolution 65/41 on developments in the field of information and telecommunications in the context of international security.

Australia aspires to be a world leader in cybersecurity. We recognize the importance and benefits of the advances in technology to the global digital economy and the security of all nations. Australia aims to maximize economic and security gains for all nations as a result of our expertise.

As technologies have become more pervasive in our lives, Government, business and individuals have become increasingly dependent upon them for a variety of purposes and functions, ranging from online purchasing of goods and services, communicating with others, searching for information and managing finances through to controlling equipment in the mining and manufacturing industries. To maximize the benefits of the Internet and the digital economy, and to enhance cybersecurity around the globe, it is imperative nations work together to achieve a trusted, secure and resilient cyberspace. Australia strives to be a proactive and engaged player in enhancing cyberspace for all users — States, business and individuals.

[1] A/65/201.

General appreciation of the issues of information security

Australia recognizes cybersecurity as a top-tier national security priority. The global community continues to experience an increase in the scale, sophistication and successful perpetration of cybercrime. As the quantity and value of electronic information has increased, so too have the efforts of criminals and other malicious actors who have embraced the Internet as a more anonymous, convenient and profitable way of carrying on their activities.

Confronting and managing these risks must be balanced against individual civil liberties, including the right to privacy, and the need to promote efficiency and innovation to ensure that Australia realizes the full potential of the digital economy.

Australia's, and each individual nation's, national security, economic prosperity and social well-being are critically dependent upon the availability, integrity and confidentiality of a range of information and communications technologies. In response, the Australian Government has committed significant resources to proactively promote the maintenance of a trusted, secure and resilient electronic operating environment for the benefit of all users.

While the Australian Government's cybersecurity policy is primarily concerned with the availability, integrity and confidentiality of Australia's information and communications technologies, it is coordinated with those of other related policies and programmes such as cybersafety, which is focused on protecting individuals, especially children, from offensive content, bullying, stalking or "grooming" online for the purposes of sexual exploitation.

Efforts taken at the national level to strengthen information security and promote international cooperation in the field

Domestic efforts to strengthen information security

Australia recognizes that it must model best practice domestically to be able to promote international cooperation in cyberspace. Australia has a government-led, integrated approach to protecting and strengthening cybersecurity. In 2009, the Government released its inaugural cybersecurity strategy that articulates the overall aim and objectives of the Australian Government's cybersecurity policy and sets out the strategic priorities that the Australian Government will pursue to achieve these objectives. The strategy also describes the key actions and measures that will be undertaken through a comprehensive body of work across the Australian Government to achieve these strategic priorities.

The aim of Australia's cybersecurity policy is to maintain a trusted, secure and resilient electronic operating environment that supports Australia's national security and maximizes the benefits of the digital economy. Key initiatives of the strategy include the establishment of two mutually supporting organizations: a new national computer emergency response team and the Cyber Security Operations Centre. Established in 2010, the computer emergency response team provides a single point of contact for cybersecurity information for all Australians and Australian businesses and ensures that Australian Internet users have access to information on cyberthreats, vulnerabilities in their systems and information on how to better protect their information and communications technologies. The team maintains close working relationships with owners and operators of critical infrastructure and businesses that operate systems important to Australia's national interest. It provides

these businesses with targeted information about cybersecurity threats and vulnerability to assist in better protecting their information and communications technologies infrastructure. The operations centre, also established in 2010, provides the Australian Government with all-source cybersituational awareness and an enhanced ability to facilitate operational responses to cybersecurity events of national importance. The Centre identifies and analyses sophisticated cyberattacks and assists in responding to cyberevents across government and critical private sector systems and infrastructure.

A key priority of the strategy is to educate and empower all Australians with the information, confidence and practical tools to protect themselves online. The strategy is guided by the principle of shared responsibility where all users, in enjoying the benefits of information and communications technologies, should take reasonable steps to secure their own systems, should exercise care in the communication and storage of sensitive information and have an obligation to respect the information and systems of other users. To enable individuals to play an active role in information security, it is essential individuals maintain an awareness and understanding of the cyberenvironment and its risks. To achieve this, Australia has an ongoing programme of awareness-raising, which includes a website for cybersecurity information for Australian home users and small businesses, including for those with limited cyberknowledge and skills (see www.staysmartonline.gov.au) and a cybersecurity awareness week conducted in partnership with business, consumer groups and community organizations. The awareness week helps Australians to understand cybersecurity risks and educates home and small business users on the simple steps they can take to protect their personal and financial information online. During the 2010 National Cyber Security Awareness Week around 150 government agencies, industry, community and consumer organizations partnered to deliver events and activities in metropolitan, regional and rural Australia. In 2011, the awareness week was held from 30 May to 4 June.

In acknowledging that the security of cyberspace is a shared responsibility, the Australian Government has worked proactively with the Internet Industry Association to develop an innovative voluntary Internet service provider cybersecurity code of practice (the "icode"), which commenced in December 2010. The code provides a consistent approach for Australian Internet service providers to help inform, educate and protect their clients in relation to cybersecurity issues. Australia has presented on the successful implementation of the code and shared its lessons learned from developing this code in multilateral forums. Presentations have been made in the Organization for Economic Cooperation and Development (OECD) Working Party on Information Security and Privacy in December 2010, the Asia-Pacific Economic Cooperation (APEC) Telecommunications and Information Working Group and the Asia-Pacific Telecommunity. Australia is eager to share this code with other States, through bilateral capacity-building exercises and multilateral forums, to assist other States in better collaborating with Internet service providers and to make those providers more responsible for educating and protecting end-users.

Promotion of international cooperation

Australia gives high priority to international cooperation on cybersecurity. Given the transnational nature of the Internet, in which effective cybersecurity requires coordinated global action, Australia has adopted an active, multilayered

approach to international engagement. This includes, among other things, engaging with foreign Governments and organizations bilaterally and via multilateral forums to help promote international best practice, share lessons, build capacity and foster a coordinated global approach to combating cybersecurity threats.

Australia's involvement in the United Nations includes co-sponsoring resolutions on the creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures, and on developments in the field of information and telecommunications in the context of international security. Australia has also responded to General Assembly resolution 64/211 by providing input on best practices for the protection of critical information infrastructure, including information and communications technologies, with a view to promoting global improvement in cybersecurity. Australia is a member of the International Telecommunication Union (ITU), and contributes to study groups under the Standardization and Development sectors. Australia provides funding to the Development sector for capacity-building work in the Asia and Pacific region, including cybersecurity initiatives. Australia is an active contributor to and the previous Chair of the OECD Working Party on Information Security and Privacy, and currently a volunteer country for the Working Party's comparative analysis of cybersecurity strategies. Australia was an integral leader in the development and implementation of the Seoul-Melbourne Anti-Spam Agreement on cooperation between Asia-Pacific nations in countering spam and the London Action Plan, which is the pre-eminent international enforcement and cooperation network for combating spam.

Australia enjoys a collaborative relationship and is committed to working with its regional partners. We are closely engaged with other countries in our region in building capacity to achieve a trusted, resilient and secure cyberspace. Australia participates in activities of the Asia-Pacific Economic Cooperation Telecommunications and Information Working Group (APEC TEL) and the Association of Southeast Asian Nations (ASEAN) Regional Forum work on cybersecurity. Australia is the deputy convenor for the APEC TEL Security and Prosperity Steering Group. Australia is currently seeking to co-lead the cyberterrorism and transnational crime core area under the ASEAN Regional Forum workplan.

At an operational level, the computer emergency response team maintains close working relationships with national computer emergency response team organizations around the globe. In Australia, the team actively participates in and facilitates trusted and timely information sharing on a global level, including threat and vulnerability information, to ensure the maintenance of situational awareness and a consistent and coordinated global response to online threats. The team actively contributes to capacity-building initiatives, particularly in the Asia-Pacific region, including through its membership of the Asia-Pacific Computer Emergency Response Team. Recognizing that information security is not geographically limited, the team also works closely with other partners through its membership of the Forum of Incident Response and Security Teams and the International Watch and Warning Network.

Possible measures that could be taken by the international community to strengthen information security at the global level

All States, including Australia, need to continue to seek out both traditional and innovative measures to strengthen information security. The global challenge of cybersecurity requires an increased effort in multilateral forums to improve the security of interoperable networks. This includes efforts within the United Nations and the ITU, regional forums such as APEC and more subject specific international groups such as the Forum of Incident Response and Security Teams and the International Watch and Warning Network.

Australia supports the development of international principles of responsible behaviour in cyberspace, including agreeing a broad set of principles for normative behaviour in cyberspace that will facilitate better international cooperation and promote trust in cyberspace and lead to the development of agreed international norms on cyberspace. Australia, as a member of the global community, will continue to support progress on this issue through bilateral and multilateral forums to help achieve a more secure, resilient and trusted cyberenvironment.

Specific efforts that could be taken by the international community to strengthen information security at the global level include:

(a) The development of global standards, including agreement to a broad set of international principles for normative behaviour in cyberspace to facilitate better international cooperation and promote trust;

(b) Expansion of the international legal system's capacity to combat cybercrime, including consistency in legal frameworks (for example, wider accession to the Council of Europe Cybercrime Convention, the requirements of which Australia anticipates to meet by the end of 2011), and enhancing law enforcement cooperation to allow countries to effectively institute domestic law;

(c) The development and promotion of best practice in situational awareness and strategic warning and event response, including the development of national computer emergency response teams to conduct and coordinate these activities between all nations;

(d) Awareness-raising initiatives and capacity-building exercises by experienced and established States to assist developing States to achieve a trusted, secure and resilient cyberspace for the benefit of all;

(e) A more consistent approach to partnering with industry to develop guidelines around conduct in cyberspace, for example, the Australian Internet industry code of practice.

Relevant international concepts

Existing international law provides a framework for protection from information security threats arising from a variety of actors. A range of existing international legal principles may be applicable to the use of cyberspace, including the principles of sovereign equality of States and the prohibition on the use of force and acts of aggression, as well as international humanitarian law. Further discussion among States, in international and regional forums, is necessary to determine more precisely the scope and applicability of these principles to threats emanating from the cyber realm.

Georgia

[Original: English]
[1 June 2011]

In the context of Georgia, the information security issues were given particular attention after August 2008, when the Russian Federation carried out a heavy distributed denial-of-service attack against Georgia.

Given the assessment of these events and under the recent rapid and large-scale development of e-governance projects and services, information security has become one of the significant aspects of the national security concept. For the improved regulation of information security, the Government of Georgia has been carrying out a number of significant initiatives in recent years.

In 2010, a legal entity, the Data Exchange Agency, was established under the Ministry of Justice of Georgia, which is directly responsible for the development and implementation of information security policy in the Government sector. With the establishment of the Data Exchange Agency, the Government of Georgia has developed the institutional mechanism for coordinated realization of e-governance and information security.

The Data Exchange Agency, within the framework of functions provided for by the law and its own charter, cooperates with the Ministry of Justice of Georgia in pursuing and introducing of an information security policy, which should conform to International Organization for Standardization (ISO) 27000 standard. The Agency also coordinates the enforcement and introduction of either mechanisms or standards necessary for information security in the State and business sectors, particularly by carrying out activities of various levels of significance. Out of these events, one the most important is the annual Georgian information technology innovations conference, the agenda of which always deals with information and cybersecurity; the conference also has the mandate of the Agency to develop and carry out the policy of public awareness enhancement regarding information and cybersecurity issues.

In the context of everyday cybersecurity, the Data Exchange Agency is responsible for the establishment and operation of the computer emergency response team, which currently is functioning at the Agency with a view to managing the information security incidents in Georgia's cyberspace. The Agency also monitors the functioning of the Georgian governmental network for the safeguarding of its security.

The functions of the Agency, in the context of information and communication technologies, also provide for raising the levels of professional education (in order to train information security specialists), preparing proposals, monitoring security and issuing digital signature certificates. Given the sphere of professional education, the Agency plans to carry out a number of special projects with the help of international donors (such as the European Union (EU) and the World Bank). These projects will ensure the appropriate level of professional education; as for digital signature security, the Agency will perform this function upon the beginning of issuance of citizens electronic identity cards (bearing digital signatures) by the Civil Registry Agency.

Besides the activity of the Data Exchange Agency, which is the leading and coordinating agency for information security, one should underline other initiatives carried out currently by the Government of Georgia, in which the Data Exchange Agency is actively engaged:

(a) The expert working group, which is working on the cybersecurity strategy and action plan (defined concretely in the next part), has been established under the National Security Council of Georgia;

(b) A number of legislative initiatives have been developing, including the administrative law and the law regulating State secrets, which are planned to be initiated at the Parliament of Georgia in 2011. One should make special mention of the Bill on information security, which is currently being developed by the Data Exchange Agency and is to be submitted for consideration by the Parliament in 2011;

(c) In 2010, the Ministry of Justice and the Ministry of Finance of Georgia, with the help of the Agency, developed and are now introducing information security internal regulations (policy and guidelines). Similar initiatives are also expected to be implemented in other governmental institutions.

Germany

[Original: English]
[6 June 2011]

The security situation in cyberspace has fundamentally changed over recent years. On the one hand, we can see a technology-driven process of innovation at work, as more and more business processes are managed electronically and interconnected, sometimes directly or indirectly connected to the Internet. Information technology systems are constantly becoming more complex. Innovation cycles are getting shorter and shorter. On the other hand, organized crime and other non-state actors are attacking information technology networks, databases and websites. In some cases, these attacks are having impacts that have not yet been realistically assessed.

For this reason, in February 2011 the Federal Government adopted a new cybersecurity strategy. The core of the strategy is critical infrastructure protection. All Government authorities that deal with cybersecurity issues are to work closely and directly with each other and with the private sector within a new cyber response centre to rapidly detect and analyse major information technology incidents and recommend protective measures. With regard to policy, the new Cyber Security Council at the State secretary level addresses key cybersecurity issues and Germany's position on them.

This includes coordinating cyber foreign policy, including aspects of foreign, defence, economic and security policy. International interconnections in cyberspace mean that coordinated action at the international level is essential. Within the EU and in international organizations, Germany will therefore strongly advocate greater cybersecurity.

In its cybersecurity strategy, in view of the global interconnection of information technology, Germany advocates developing broad, non-contentious,

politically binding norms of State behaviour in cyberspace. They should be acceptable to a large part of the international community and should include measures to build trust and increase security.

Confidence and security-building measures in cyberspace

Cyberspace is a public good and a public space. As such we have to consider cyberspace security in terms of the resilience of infrastructure as well as the integrity and failure safety of systems and data. Being a public space, States have to promote security in cyberspace, particularly regarding security against crime and malicious activities, by protecting those who choose to use authenticity tools against identity theft and securing the integrity and confidentiality of data and networks.

Cyberspace is global by nature. Ensuring cybersecurity, enforcing rights and protecting critical information infrastructures require major efforts by the State both at the national level and in cooperation with international partners.

Against this backdrop, Germany is ready to work on a set of behavioural norms addressing State-to-State behaviour in cyberspace, including, in particular, confidence, transparency- and security-building measures, to be signed by as many countries as possible.

Germany outlined possible elements of such a code of conduct on international norms recently at the Organization for Security and Cooperation in Europe (OSCE) conference on cybersecurity, held on 9 and 10 May 2011, as follows:

(a) Confirm the general principles of availability, confidentiality, competitiveness, integrity and authenticity of data and networks, privacy and protection of intellectual property rights;

(b) Respect the obligation to protect critical infrastructures;

(c) Enhance cooperation aiming at confidence-building, risk reducing measures, transparency and stability by:

- Exchanges of national strategies, best practices and national perceptions referring to the international regulation of cyberspace;
- The exchange of national views of international legal norms pertaining to the use of cyberspace;
- The setup and notification of points of contact;
- The setup of early warning mechanisms and the enhancement of cooperation between computer emergency response teams;
- The upgrade of crisis communication links to encompass cyberincidents, the support of the development of technical recommendations that advance robust and secure global cyberinfrastructures;
- The responsibility to combat terrorism comprising the exchange of practices and enhanced cooperation to address non-State actors;
- The support of cybersecurity capacity-building in developing countries, and the development of voluntary measures for cybersecurity support to large-scale events (e.g. the Olympic Games).

Moreover we see the necessity to start a debate on an international cooperation in the framework of attribution of cyberattacks, which are usually very difficult to trace, State responsibility for cyberattacks launched from their territory when States do nothing to end such attacks despite being informed about them and States' responsibility not to facilitate areas of lawlessness in cyberspace, for example by knowingly tolerating the storage of illegally collected personal data on their territory.

Military aspects of cybersecurity

As military forces increasingly rely on information technology to master ever more complex scenarios at all levels of command, the protection of the information and the means to process it has become a first order task.

However, in military thinking, information security is challenged not only by a potential adversary, in an operational understanding, using weaponry for the physical destruction of information infrastructure, but also by irresponsible users, malfunctioning technology, criminals or simply accidents.

Hence, the efforts to be undertaken range from awareness-raising of each single user and securing the trustworthiness of the supply chain for information technology, to responsive defences to fend off cyberattacks and an overall resilient information technology architecture.

In essence, a comprehensive risk management is required, with measures to strengthen information security on a national and global scale.

At an early stage, the German armed forces (Bundeswehr) established resilient command and control architectures, security techniques and procedures as well as an information technology-security organization, encompassing all branches of the armed forces, and including an independent computer emergency response team with the capacity to intervene in case of critical disruptions to the operations of information technology. Adapting personal and technical abilities to the continually increasing level of threat is a perpetual task.

The German armed forces are collaborating closely with the Federal German Ministry of the Interior in its efforts and strongly support the strengthening of information security in the North Atlantic Treaty Organization (NATO) and the EU and the formation of policies and capacities to this end. Furthermore, the armed forces hold regular exchanges with a number of countries in the context of information security, both at the policy and working levels.

The German armed forces welcome initiatives and work together with other departments of the Federal German Government on international motions to further protect the utility of worldwide information networks, for example, the development of a voluntary international code of conduct in cyberspace.

Cyberdefence in NATO

Cybersecurity has been identified by NATO as one of the key emerging security challenges. The Strategic Concept adopted by Heads of State and Government at the NATO Summit, held in November 2010, in Lisbon, states that "cyber attacks ... can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability".

Heads of State and Government tasked the North Atlantic Council, in the Summit Declaration, "to develop, drawing notably on existing international structures and on the basis of a review of our current policy, a NATO in-depth cyberdefence policy by June 2011 and to prepare an action plan for its implementation".

As a first step to the new policy, NATO Defence Ministers adopted a concept on cyberdefence in March 2011.

The concept focuses on the protection of NATO networks and national networks of member States that are connected to NATO networks or process NATO information (including the development of common principles and criteria to ensure a minimum level of cyberdefence in all member States). To reduce the global risks emanating from cyberspace, NATO intends to cooperate with partner nations, relevant international bodies such as the United Nations and the European Union, the private sector and academia.

- Germany welcomes NATO commitment regarding cybersecurity and actively supports the discussions.

Cybersecurity in the Organization for Security and Cooperation in Europe

The Organization for Security and Cooperation in Europe has been discussing cybersecurity issues for several years. At the OSCE Summit held in 2010, in Astana, the Heads of State and Government of the 56 participating States of the OSCE underlined that "greater unity of purpose and action in facing emerging transnational threats" must be achieved. The Astana Commemorative Declaration mentioned cyberthreats as one of these emerging transnational threats.

Germany actively participated in the OSCE conference on a comprehensive approach to cybersecurity: "Exploring the future OSCE role", held on 9 and 10 May 2011, in Vienna. In the course of the conference, concrete recommendations for OSCE follow-up activities were discussed.

Germany will continue to actively support OSCE discussions on exploring the future OSCE role in the field of cybersecurity.

Greece

[Original: English]
[6 June 2011]

Information security issues have been more extensively addressed than in the past. Counter-measures to the threats inherent in the current globalization of networks and systems are being considered. Measures to preserve the free flow of information are studied and applied in both the national and international contexts.

Current international and multinational concepts are followed and studied. International guidance on risk assessment is needed. Cyberdefence should also be addressed. National sovereignty rights regarding information security in global information sharing should be maintained.

It is understood that all Member States should continue to inform the Secretary-General of their views and assessments on the corresponding questions. In this respect the following points are noted:

(a) All information security-related issues are given high priority;

(b) Ways to preserve the free flow of information and provide for the required degrees of confidentiality, integrity and availability are studied and applied across national and international boundaries;

(c) The concepts for the interconnection of networks that provide for capabilities enabled and shared at both the national and international levels should be drafted and agreed. Risk assessment for the interconnection of networks must prevail and relevant international guidance should be available. Further to that, and since a very serious concern for every nation has been the need to take measures for its cyberdefence, coherent international guidance is needed for cooperation, efficiency and economy. Last but not least, the requirement for a nation to preserve its sovereignty and maintain its own base of information cannot be overlooked and every concept drafted should account for that;

(d) Possible measures to be taken by the international community to strengthen information security at the global level are the following:

(i) Relevant international concepts should be detailed and agreed;

(ii) A guidance plan for a harmonized generic infrastructure, covering basic legislation matters, could be proposed, in order to deliver the required information security for the electronic handling of all correspondence and messaging, providing multiple ways of communication;

(iii) Concepts followed by multinational alliances and groupings of small nations should be harmonized and expanded to be applicable at the global level. The agreement to specify the threat and its negative effect on humanity could be more important than the engineering of any sophisticated measures devised, since they could also be used by adversaries;

(iv) In parallel to all of the above, the nation's sovereignty should be understood to be the basic reference for every attempt of globalization. An international concept for defining the national information exchange gateways, with scenarios reflecting the desired level of integration, should be drafted and used as a guide, for all efforts at the national, multinational and international levels.

Kazakhstan

[Original: Russian]
[7 June 2011]

In 2010, the Republic of Kazakhstan set up a computer emergency response team to ensure cybersecurity for information and communications technologies.

In this connection, any information received from Kaznet users on viruses, security codes, bot systems or violations of legal requirements (pornography, violence, copyright infringements and so on) detected in the kz domain or on sites hosted by Kazkhstan is sent to the computer emergency response team for analysis.

Netherlands

[Original: English]
[6 June 2011]

General appreciation of the issues of information security

The Netherlands supports safe and reliable information and communications technologies and the protection of an open, free Internet and respect for human rights. Safe and reliable information and communications technologies are essential for our prosperity and well-being and serve as a catalyst for sustainable economic growth.

Information and communications technologies offer opportunities, but also make our society more vulnerable. The cross-border nature of threats makes international cooperation crucial. Many measures will be effective only if implemented or coordinated internationally. In this connection, the Netherlands attaches great importance to public-private partnerships and individual responsibility on the part of all users of information and communications technologies.

Efforts taken at the national level to strengthen information security and promote international cooperation in the field

The Netherlands is working nationally and internationally for a secure digital environment. At the national level, in February 2011, the Dutch Government presented a national cybersecurity strategy, entitled "Strength through cooperation". In July 2011, as part of the strategy, the Government will establish a national cybersecurity council to ensure a collaborative approach between the public sector, the private sector and academic and research institutions. The Government will also establish a national cybersecurity centre to identify trends and threats and help manage incidents and crises. A major task of the centre will be to conduct cyberthreat analyses based on information from public and private parties. The centre will include the existing Government computer emergency response team.

Internationally, the Netherlands contributes actively to the efforts of EU, NATO, the Internet Governance Forum, ITU and other partnerships. The Netherlands promotes practical cooperation between cybersecurity centres (including computer emergency response team organizations) and a strengthening of the International Watch and Warning Network. The rapid growth in cybercrime calls for effective enforcement to maintain confidence in the digital society. As to enforcement, the Netherlands aims to encourage more cross-border investigation with enforcement agencies from other European countries, and beyond. The Netherlands is a party to the Council of Europe's Convention on Cybercrime and encourages others to accede to this convention.

Possible measures that could be taken by the international community to strengthen information security at the global level

The Netherlands realizes the importance of continuing dialogue on the development of standards of State behaviour aimed at the safe use of cyberspace. It is keen to contribute actively to this dialogue. The Netherlands' starting point is an

open Internet that promotes innovation, stimulates economic growth and safeguards fundamental freedoms.

The Netherlands attaches great importance to involving the private sector and knowledge institutions in this dialogue and is keen to share experience and best practices with others. The intensive international exchange of knowledge and information among all stakeholders and organizations is essential for making cyberspace more secure and reliable. Consistency in the application of existing international legal frameworks is another important issue meriting international attention.

United States of America

[Original: English]
[7 June 2011]

I. Introduction

Information and communications technologies are crucial to the development of all Member States. Linked together to create a cyberspace, these technologies help to realize the common vision of an information society as envisaged at the World Summit on the Information Society, held in 2003 and 2005. Information and communications technologies contribute to the essential functions of daily life, to commerce and the provision of goods and services, research, innovation, entrepreneurship, and to the free flow of information among individuals, organizations and Governments. They are a powerful new tool, allowing e-government, promoting economic development, facilitating the delivery of humanitarian assistance and enabling critical civil, public safety and national security infrastructures. Moreover, the promise that networked communications offer to reduce barriers to international understanding and cooperation cannot be overstated.

Even as reliance on information and communications technologies grows, risks associated with this dependency grow as well. A diverse range of events and activities, natural and man-made, threaten the reliable functioning of critical national infrastructures, global networks and the integrity of the information that travels over or is stored within them. Man-made threats are increasing in number, sophistication and gravity. Some are State-based, but many come from non-State actors and involve criminal or terrorist activity. Motivations vary, from the theft of money or information, or the disruption of competitors, to nationalism and the extension of traditional forms of State conflict into cyberspace. These threat actors target individuals, corporations, critical national infrastructures and Governments alike, and their effects carry significant consequences for the welfare and security of individual nations and the globally linked international community as a whole.

Whatever national steps Governments may take domestically to protect their information networks, international collaboration on strategies to reduce risks to information and communications technologies is essential to ensure the security of all. Governments must have confidence that the networks that support their national security and economic prosperity are safe and resilient. Achieving a trusted infrastructure for information and communications technologies will ensure that all achieve the potential of the information revolution.

That task will not be easy. The international community faces the challenge of maintaining an environment that promotes efficiency, innovation, economic prosperity and free trade while also promoting safety, security, civil liberties and privacy rights. The difficulty of the task is compounded by the unique attributes of information and communications technologies. Accessible to all, networks are often owned and operated by the private sector, rather than by Governments. Unlike traditional weapons, disruptive information technology tools are stealthy and cannot be seen. Their use can be routed through many nations, with the origin, identity and sponsorship of the perpetrator difficult to determine. Increasingly, non-State actors are developing capabilities that raise the possibility of States or non-State actors using proxies to engage in disruptive activities in cyberspace. These attributes make traditional strategies, such as measures similar to those used for arms control, ineffective in controlling or constraining threat actors and therefore, creative new approaches are required to mitigate the risks. Notwithstanding the difficulty of the task, Member States must unite in the common goal of preserving and enhancing the contribution that information technologies make by assuring their security and integrity.

The tasks of Member States are twofold: domestic and international. Securing national information infrastructures is a responsibility Governments must lead on domestically, in coordination with relevant civil society stakeholders. At the same time, domestic efforts should be supported by international collaboration on strategies that address the transnational nature of the various threats to networked information systems. These efforts should include cooperation on incident management, mitigation and response; transnational criminal investigation and prosecution; technical recommendations to improve the robustness of cyberinfrastructure; and affirmation of internationally shared norms of behaviour supported by confidence-building measures designed to enhance stability and reduce risks of misperception.

II. Threats, risks, vulnerabilities

Threats to the network of systems that together constitute cyberspace, and the information that travels over them, is one of the serious global challenges of the twenty-first century. State and non-State actors can target ordinary citizens, commerce, critical industrial infrastructures and Governments through information and communications technologies. The convergence between information and communications technologies, the Internet and other infrastructures creates unprecedented opportunities to cripple telecommunications, electrical power, pipelines and refineries, financial networks and other critical infrastructures.

The unique characteristics of information technology facilitate its use for disruptive activities and severely challenge Governments that seek to reduce risk. Unlike traditional military technologies, the networks that constitute cyberspace are not the monopoly of Governments, but are in many cases owned and operated by the private sector. Information technology itself is a widely available technology that is neither inherently civil nor military in nature, where its use depends exclusively on the motivation of the user.

Software tools used for disruption, at least in their basics, are freely available to all. More sophisticated approaches can be developed by anyone with the requisite skill. Moreover, these tools evolve rapidly to take advantage of newly discovered

vulnerabilities. Such tools are not visible in the conventional sense, are quite stealthy and may have latent "signatures" that can be easily mimicked. Because of the nature of the Internet, malicious code can be routed through many national territories before delivery to target, making identification of their origin onerous, time-consuming and often requiring substantial transnational cooperation. Even if their origin is discovered, the identity of the perpetrator or the sponsors can remain elusive. Consequently, malicious actors can and do operate in secrecy, with substantial impunity, from virtually anywhere on the planet.

This obscurity of identity is compounded by an obscurity of the motive underlying an intrusion in cyberspace. Organized criminals and other individuals or groups may act to advance their own interests but also can be enlisted to serve as proxies by both State and non-State actors alike. The lack of timely, high-confidence attribution and the possibility of "spoofing" can create uncertainty and confusion for Governments, thus increasing the potential for crisis instability, misdirected responses and loss of escalation control during major cyberincidents.

The primary actors that together constitute threats to the reliable functioning of cyberspace include:

(a) **Criminals**. Many of the malicious tools originate in the entrepreneurial efforts of organized criminals and hackers. The growing sophistication and scope of criminal activity highlight the potential for malicious activity in cyberspace to affect national competitiveness, to cause a general erosion of trust in the use of the Internet for commerce and trade, even to cripple civil infrastructure. The volume and scope of such activities are increasing;

(b) **States**. There is increased anecdotal public reporting that States are developing and using capabilities that extend traditional forms of state conflict into, using, or through cyberspace. However, conclusive evidence regarding the source or intentions behind events commonly assumed to be State-sponsored remains elusive. As is often the case, the identity and motivation of the perpetrator(s) can only be inferred from the target, effects and other circumstantial evidence surrounding an incident;

(c) **Terrorists**. Terrorist capability to compromise information networks or to execute operations with physical effects through the use of information and communications technologies is currently lacking, although the possibility that such capabilities may emerge in the future cannot be ruled out. Most experts agree that, currently, terrorists rely on information and communications technologies to recruit, to organize and to solicit funding. Specific threats arising from terrorist use of the Internet may include use of the Internet for organizing and carrying out a specific kinetic terrorist attack;

(d) **Proxies**. Of increasing concern are individuals or groups who engage in malicious online activities on behalf of others, whether State or non-State actors, for financial gain or for nationalist or other political motivation. So-called "bot-masters" are reported to offer various malicious services to the highest bidder. The unique attributes of information technology offer a high degree of anonymity to such actors and effectively obscure any relationship to a sponsor, offering the sponsor plausible deniability.

The challenges States face in addressing such threats are formidable. The attributes of information and communications technologies mean that the actions of

each of these threat actors are likely visible only in their effects. Thus, high-confidence attribution of identity to perpetrators cannot be achieved in a timely manner, if ever, and success often depends on a high degree of transnational cooperation. The increasing role of proxies further complicates the process of attribution, as an affected party must identify not only the perpetrator but also the sponsor, promising to make this challenge even more troublesome in the future.

Such challenges require that national Governments organize and lead domestic efforts to develop and deploy resilient, layered defences for communications and information infrastructures, regardless of the source of the threat. At the same time, the complex transnational nature of these threats requires international collaboration on strategies to address risks on a global basis.

III. Principles, rules and norms of behaviour

A. Responsibilities of States in assuring cybersecurity

Over the past decade, Member States have recognized their national responsibility to take systematic domestic steps to defend themselves from cybersecurity threats and have affirmed the need for international cooperation. Five General Assembly resolutions have drawn attention to essential defensive measures that Governments can perform to reduce risks to their security. While intended to raise awareness, these resolutions nonetheless advance some useful norms for individual and State behaviour in the interest of cybersecurity:

(a) Resolution 55/63 on combating the criminal misuse of information technologies, in which the General Assembly underscores the need to have modern effective national laws to adequately prosecute cybercrime and facilitate timely transnational investigative cooperation;

(b) Resolution 56/21, in which the General Assembly specifically notes the work of international and regional organizations in combating high-technology crime, including the work of the Council of Europe in elaborating the Convention on Cybercrime:

> There has been intensive activity by the United Nations and other organizations in this area. United Nations organizations that principally focus on criminal misuse of the Internet include the United Nations Office on Drugs and Crime, the Commission on Crime Prevention and Criminal Justice, the United Nations Congress on Crime Prevention and Criminal Justice, the International Telecommunication Union and others;

(c) Resolution 57/239, in which the General Assembly affirms the need for the creation of a global culture of cybersecurity, recognizes the responsibility of Governments to lead all elements of society to understand their roles and responsibilities with regard to cybersecurity, and highlights complementary elements that all participants in the information society must address;

(d) Resolution 58/199, in which the General Assembly focuses in particular on actions that Member States should consider in their efforts to create a global culture of cybersecurity and to protect critical information infrastructures. These too can be considered a set of norms to which Governments should ascribe, and they provide an essential basis or precursor in order to facilitate international collaboration on risk reduction;

(c) Resolution 64/211, in which the General Assembly invited all Member States to take detailed stock of their national cybersecurity efforts to date, in the above areas as well as others, using an annexed self-assessment tool, and to share those successful measures and best practices that could assist other Member States in their efforts.

B. Norms applicable in the context of hostilities

Despite the unique attributes of information and communications technologies, existing principles of international law serve as the appropriate framework within which to identify and analyse the rules and norms of behaviour that should govern the use of cyberspace in connection with hostilities. There are two distinct but related bodies of law to consider in this regard: *jus ad bellum* and *jus in bello*. The first provides the framework for considering whether an incident in cyberspace rises to the level of a use of force triggering a nation's right to self-defence. The second provides the framework for identifying the rules governing the use of cyberspace in the context of an armed conflict.

Jus ad bellum. Much of the legal framework governing the use of force and self-defence is derived from three provisions of the Charter of the United Nations:

(a) Article 2(4) of the Charter provides that "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state …";

(b) Article 39 of the Charter establishes the Security Council as the arbiter of whether a threat to the peace, breaches of the peace, or acts of aggression have occurred, and charges the Security Council with making recommendations or decisions as to what measures under Articles 41 or 42 of the Charter are appropriate in response;

(c) Article 51 of the Charter recognizes and reinforces the principle that "[n]othing in the present Charter shall impair the right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security".

It may be difficult to reach a definitive legal conclusion as to whether a disruptive activity in cyberspace constitutes an armed attack triggering the right to self-defence. For example, where the threat actor and the motive are unknown, and effects result that do not directly cause substantial death or physical destruction, it may be possible to reach differing conclusions about whether an armed attack has occurred. However, such ambiguities and room for disagreement do not suggest the need for a new legal framework specific to cyberspace. Instead, they simply reflect the challenges in applying the Charter framework that already exists in many contexts. Nevertheless, under some circumstances, a disruptive activity in cyberspace could constitute an armed attack. In that context, the following established principles would apply:

(a) The right of self-defence against an imminent or actual armed attack applies whether the attacker is a State actor or a non-State actor;

(b) The use of force in self-defence must be limited to what is necessary to address an imminent or actual armed attack and must be proportionate to the threat that is faced;

(c) States are required to take all necessary measures to ensure that their territories are not used by other States or non-State actors for purposes of armed activities, including planning, threatening, perpetrating or providing material support for armed attacks against other States and their interests.

Jus in bello. The law of armed conflict set forth the rules, known as *jus in bello*, that apply to the conduct of armed conflict, including the use of information technology tools in the context of an armed conflict. In particular, the following key principles of the law of armed conflict would play an important role in judging the legality of cyberattacks during an armed conflict:

(a) The principle of distinction requires attacks to be limited to legitimate military objectives and that civilian objects shall not be the object of attack;

(b) The prohibition on indiscriminate attacks includes a prohibition on attacks that employ a means or method of warfare that cannot be reasonably directed at a specific military objective;

(c) The principle of proportionality prohibits attacks that may be expected to cause incidental loss to civilian life, injury to civilians, or damage to civilian objects, which would be excessive in relation to the concrete and direct military advantage anticipated.

These principles prohibit attacks on purely civilian infrastructure, the disruption or destruction of which would produce no meaningful military advantage. In addition, the potential for collateral damage would have to be assessed before attacking a military target. In other words, targeting analysis would have to be conducted for information technology attacks just as it traditionally has been conducted for attacks using kinetic (conventional and strategic) weapons.

While the principles above are well-established and apply in the context of cyberspace, it is also true that interpreting these bodies of law in the context of activities in cyberspace can present new and unique challenges that will require consultation and cooperation among nations. This is not unusual. When new technologies are developed, they often present challenges for the application of existing bodies of law.

C. The use of proxies

The use of proxies to conduct disruptive operations is an example of an area where the unique attributes of information and communications technologies present new challenges for States. Acting through proxies significantly increases States' ability to engage in attacks with plausible deniability. While existing international law has provisions governing the use of mercenaries, the use of proxies in cyberspace raises new and significant issues with wide-ranging implications. States will need to work together to develop effective solutions to this problem.

D. Responsibility to allow free flow of information

The rights to freedom of expression and the free flow of information are embodied in the Universal Declaration of Human Rights and the International

Covenant on Civil and Political Rights, which generally provide, subject to certain limitations, that everyone has the right to freedom of expression, including the freedom to hold opinions without interference and to seek, receive and impart information through any media and regardless of frontiers. These principles have been affirmed in numerous international forums, including the General Assembly, the International Telecommunication Union and the World Summit on the Information Society, among others.

E. Responsibility to combat terrorism

At least 16 existing Security Council resolutions call on States to combat terrorism. These obligations apply fully when terrorists or terrorist facilitators use cyberspace to recruit, raise funds, move money, acquire weapons or plan attacks. All States are obliged to share information about, and to take action against, online terrorist financing, recruitment, planning and facilitation activities, while respecting the sovereignty of other States and their own responsibilities to allow the free flow of information.

IV. Transparency, stability and risk reduction and cooperative measures

As outlined above, Member States face the challenge of managing a highly varied and complex threat environment. Over the last decade, extensive efforts to combat the threat of cybercrime have been conducted internationally. Efforts in training in the investigation and prosecution of cybercrime have been taken up in the Organization of American States, the Asia-Pacific Economic Cooperation, the Economic Community of West African States, the African Union and the Council of Europe, among others. Extensive international cooperation in the investigation and prosecution of cybercrime has been accomplished through the Convention on Cybercrime, as well as through bilateral efforts between affected countries, and continues to be the most effective way of dealing with the threat to information and communications technologies by criminal activity.

Other areas of transnational concern have yet to receive similar attention. These include risks of misperception resulting from a lack of shared understanding regarding international norms pertaining to State behaviour in cyberspace, which could affect crisis management in the event of major cyberevents. This argues for the elaboration of measures designed to enhance cooperation and build confidence, reduce risk or enhance transparency and stability:

Transparency measures

- Exchanges of national cybersecurity strategies and best practices (lessons learned)
- Exchanges of national views of international norms governing the use of cyberspace
- Exchanges of national organizational structures devoted to cybersecurity and points of contact.

Stability and risk reduction measures

- Establishing or upgrading communications links and associated protocols to encompass cyberincidents

- Enhancing cooperation to address organized non-State actors (criminals, terrorists, proxies)
- Establishing procedures to permit routine exchange of information between national computer security incident response teams.

Cooperative measures

- Support cybersecurity capacity-building in less developed nations.